AU/ACSC/028/2002-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

SUPPORTING THE INFORMATION-CENTRIC 2001 QUADRENNIAL DEFENSE REVIEW:

THE CASE FOR AN INFORMATION SERVICE

by

Robert Costa, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Major Robert T. Childress

Maxwell Air Force Base, Alabama

April 2002

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **00 APR 2002**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE
Supporting The Information-Centric 2001 Quadrennial Defense Review: The Case For An Information Service

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air University Maxwell Air Force Base, Alabama

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**260**	

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Tables

Page

Preface

> *Achieving the objectives of the defense strategy requires the transformation of the U.S. Armed Forces. Transformation results from the exploitation of new approaches to operational concepts and capabilities, the use of old and new technologies, and new forms of organization that more effectively anticipate new or still emerging strategic and operational challenges and opportunities and that render previous methods of conducting war obsolete or subordinate.*
>
> —2001 Quadrennial Defense Review

The following substantiates this research topic's importance based on 1) the *2001 Quadrennial Defense Review Report* (QDR), 2) the fundamental tenets of Professional Military Education (PME) which support its tone and tenor, and 3) the intent of the research.

2001 QDR

Upon taking office on 11 January 2001, Secretary of Defense Donald Rumsfeld clearly articulated his intention to radically transform the *Cold-War-based* military to enable it to better deter/defeat the emerging threats of a new, dynamic world order. Despite strong criticism of his ideas on the rapid and comprehensive transformation he felt necessary to break the dogmatic mindset that might continue to handicap true evolution within the Department of Defense (DoD), his vision pervaded his first QDR. As such, the QDR is centered on the threats of information warfare and space superiority, the need to compel a true *a priori* architectural underpinning for interoperability and system-of-systems engineering with respect to Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), and the metered organizational transformation necessary to turn that vision into reality. That kind of transformation requires strategic innovation. And that kind of innovation begins at PME.

Fundamental Tenets of PME

We recently had the privilege of listening to the Honorable Newt Gingrich, former Speaker of the House, where he discussed those very tenets--transformation, vision, and innovation. Addressing the ACSC student body, he noted: "You are entering a world where you're going to have a series of really big changes and you need to be thinking at non-verbal levels, not just at rational cognitive levels. You need to think about underlying patterns."[1] He discussed the ubiquity of information and our dependence on it, proving his point by reminding us that we rarely even check our automated gas receipts.

But what if its database was corrupted or the communication links failed? What if that happened in theater? It did. On 17 Jan 1991, at the onset of Desert Storm's air war, the Eastern Pacific Defense Satellite Communications System (*EASTPAC DSCS III*) experienced a sun sensor anomaly and went off-line for six hours. And in May 1998, 40M people were left without pager, ATM, and/or cell-phone service when *Galaxy IV* (a Hughes HP601 communications satellite), permanently failed with no back-up. It's just not people that are affected anymore--systems themselves are becoming mutually dependent on each other. Iridium®, many emergency service functions, and Globalstar® all depend on GPS for the timing that synchronizes their frequency management algorithms--take down GPS, and you take down much more than just navigation. Several Low-Earth Orbit satellites as well use GPS for attitude control. Mr. Gingrich was on target--we need to think radically differently, and develop new paradigms. That's where

PME comes in.

The true goal of any PME program is to consider, test, and develop new ideas; and to apply *critical thinking*--". . . that mode of thinking . . . in which the thinker improves the quality of his or her thinking by skillfully taking charge of the **structures inherent in thinking** and imposing intellectual standards upon them [emphasis added]."[2] Defense departments the world over are simply not structured to embrace innovative ideas and question new ways of executing their awesome responsibilities on a continual basis due to the rigid, hierarchical nature required to command and control forces where people's lives and national sovereignty are continuously at stake. Those same departments therefore developed PME to debate innovation while likewise ensuring utility. PME and innovation have a long and respected synergy. Three examples follow.

Kriegsakademie. The German Army has a history of engaging advanced education in the art of war to its fullest extent moreso than has any other county. This emphasis was particularly notable in the Interwar Period (1919-1939), where a new force--air power--evolved. Germany's prestigious PME academy, the *Kriegsakademie*[3] was an

> "exclusive and rigorous three-year school where Germany's top officers were trained to embrace 'mission-type' orders to improve the innovation and efficiency of their future charges. . . . [It] stressed innovation and flexibility over mechanical, doctrinaire, 'school solutions' which had dominated training programs up to that time."[4]

And innovation was indeed key at the *Kriegsakademie*--students were ranked not only with respect to academics, but with respect to the degree of innovation (and requisite feasibility) in their solutions. "Top *Kriegsakademie* graduates joined an elite general staff corps that dominated both military planning and operations. Realistic and innovative ideas were further analyzed, critiqued and adopted."[5] In a further attempt to break traditional institutional biases against change, "the *Kriegsakademie* leadership also stressed the advantages of leveraging new technologies to the extent possible."[6] As such, the Kriegsakademie birthed German submarine warfare, the combined-armed doctrine instantiated in the concept of the *Blitzrieg*, and architected the doctrine that was largely responsible for Germany's initial devastating and rapid European domination, where Poland was overrun in two days, "the effective destruction of the Red Air Force as a fighting force"[7] was completed within three days of the German Barbarossa offensive, and France sued for peace within four weeks of the German onslaught in May 1941.

US Army Command and General Staff College. Both the US Army Command and General Staff College (USCG)[8] and the Air Corps Tactical School (ACTS), established in 1926, were fashioned in the image of the *Kriegsakademie*. That legacy began at the USCG whose

> "most important contribution to the austere interwar Army was producing **thinkers**. *In World War II*, the college concentrated on mass-producing **doers**-16,000 of them-who were specifically trained for the war in progress. There was **little uncertainty as to who the enemy would be**, where the war would be fought or **what technology would be employed**. During interwar periods, *uncertainty prevails*, so logic suggests that during such times **the Army needs thinkers who can do more than execute current doctrine.** Officers should view their profession from a broader perspective, **thus adapting more readily to the next war's unanticipated conditions** [emphasis added]**."**[9]

This passage is particularly poignant given Secretary Rumsfeld's personalized forward in the QDR after the 9/11 attacks which noted:

> "The attack on the United States and the war that has been visited upon us highlights a **fundamental** condition of our circumstances: we cannot and will not know precisely where and when America's interests will be threatened, when America will come under attack, or when Americans might die as the result of aggression. We can be clear about ***trends***, but **uncertain about events**. We can identify threats, but cannot know when or where America or its friends will be attacked [emphasis added]."[10]

Today uncertainty prevails. Today we must adapt. Today we must innovate.

Air Corps Tactical School. Like the Kriegsakademie and USCG, the intent of ACTS remained intact--

> "the focus, scope, and intent of ACTS [is] the guiding force for aviation **technology** and **doctrine development**." [The ACTS faculty realized] the lessons learned from World War I airmen seemed of minimal benefit to the development of theory or doctrine. [In WWI] airpower was used as **an auxiliary weapon**, mostly in an observation role [where] fighters worked as escorts for observation aircraft [and] bombers served as an extension of the artillery. This early application of airpower supported primarily **the defensive side of warfare**. **A new vision** of strategic airpower was needed to appreciate the offensive role of airpower in battle [emphasis added]." [11]

ACTS was founded to ensure we simply do not prepare to fight the last war. It became a "sounding board for ideas [which were] often considered controversial within the services, and its ideas and teachings often strayed from official Army policy."[12] This bears a remarkable resemblance to where *Information* is presently--for centuries an indispensable support tool as information-*in*-warfare, but now expanding to include *information warfare* itself. That Sun Tzu characterized all war as deception[13] 2500 years ago makes it no less relevant today--all war is still deception and its vector--information--has now emerged as an effective offensive *and* defensive weapon in its own right capable of simultaneously paralyzing the enemy at the tactical, operational, and strategic levels at any point on the conflict spectrum. It provides, for the first time, the very real possibility of defeating the enemy *without* engaging in force-on-force battle--the pinnacle of the art of war, according to Sun Tzu.[14] Harvesting this force requires a new thought process, innovation, and the breed of transformation demanded to meet the Secretary's vision articulated in the QDR.

Intent of the Research

This research topic is simply one possible method, albeit provocative, to achieve that vision. I assert the transformation called for in the QDR, as a result of the dynamic world environment and technological change is so pressing and so radical, it can best be achieved through radical restructure. Its requisite magnitude has precedent--the Army's air forces separated from its parent 55 years ago because the nature of warfare had changed so significantly with respect to technology and the new international dynamic. Every national instrument of power (IOP)--particularly every aspect of the military--is becoming increasingly more dependent on/vulnerable to adversary information operations. And while we have been and continue to be attacked, we are not building the infrastructure to support this evolving method of warfare. Information Operations has been stymied by a kinetic, force-on-force mindset, and while the elements--C4ISR, space operations and information operations--needed to achieve true information dominance now exist, they are handicapped by an antiquated schema of categorization which obscures their inherent synergy and therefore their true potential. Secretary Rumsfeld was likewise critical noting: "We're so conditioned as a people to think that a military campaign has to be cruise missiles and television images of airplanes dropping bombs and that's just false."[15]

Information Operations and C4ISR are simply mirror images of each other--learn to do one well, and you learn to defeat the other well. And just as land forces, air forces and sea forces expose--and then resolve--their vulnerabilities through perfecting their offenses, so too will these two disciplines support each other's mutual defensive and offensive capabilities, if only they can be integrated.[16]

I only ask that the reader start with a 'clean-sheet-of-paper-mentality', and develop with me, using the Mission Needs Analysis[17] that regulates all new major acquisitions, the optimal construct to defeat a new enemy, disciplined only by the same constructs that underpin all five services--capabilities, core competencies, tenets, and doctrine. Each service has core capabilities, which, when integrated, become core competencies, in turn integrated into fundamental tenets, which support the venerable Principles of War.[18]

LtCol Joseph Reynolds, the director for the Airpower Studies Course in ACSC-02, emphasized that "the ACSC environment is essentially non-threatening; therefore, the opportunity to discipline one's mind through inquiry is a plum ripe for picking. The Airpower Studies …course's aim is not to reside at the lower levels of cognitive challenge. Instead, the course aims to inspire each student to reach higher levels of learning through personal application . . . while gaining an appreciation for **the relationship between evolving airpower thought and military effectiveness** [emphasis added]."[19]

The single most important lesson I learned from LtCol Reynold's course was that the Air Force, despite being *successful*, has not been *efficient*, consistently returning to unsubstantiated (and in fact refuted) dogma centered on a desperate "search for Douhet." My goal is simply to ask the reader to think about information differently--to break that dogmatic thinking, and if a new service does not emerge, at least for readers to recognize the weapon that *Information* has become and how inefficiently we build and wield that weapon. I make a convincing argument by showing that an Information Service actually encompasses analogous attributes each of the five current services already execute for their own environments--Land, Sea, Coastal, Littoral, and Air. I did not mistakenly neglect the space environment currently under the Air Force's purview. Space, I will successfully argue, is only a medium for information and as such, should instead fall under the Information Service's purview.

A separate service--any separate service--with its commensurate redundancies, bureaucracies, presumed cost, and the need to overcome the tremendous inertia necessary to apportion/re-assign people, funds, and resources, may indeed appear an implausible topic, no matter what the role that new service would execute--be it a separate *Space* Service, a separate *Submarine* Service, a separate *Homeland Defense* Service or a separate *Information* Service. Changing attitudes takes time. (In fact, the Army was still debating the need for a separate Air Force in the 1970's.) The topic may in fact appear too obtuse to warrant serious intellectual excursion. After all, the services have been struggling with the concept of the next apparent separate service--a Space Force for two decades. Recent significant DoD organizational changes provide the institutional underpinnings required to slowly conceive such a Space Force. These changes include: designating the USAF as the executive agent for space; elevating the position of the Undersecretary of the USAF to the position as the Space Acquisition Executive (dual-hatted as the Director of the National Reconnaissance Office (NRO)); and the creation of a 4-star billet (the first ever non-rated 4-star billet) for Air Force Space Command (AFSPC), to be commanded by Gen(S) Lance W. Lord. In addition, as Col Steven Chiabotti, Dean at the School for Advanced Airpower Studies also cautioned, taking on such a subject could be interpreted as biased, or even self-serving. As an Airman first, an officer second, and a space specialist third, one may presume I have a vested interest in breaking out into a separate service, whether information or space, given my service's dominant leadership calculus. That certainly could be the interpretation, albeit an incorrect one. I acknowledge the criticism.

So why consider the subject at all? Because Information has changed, and our dogmatic conscripts on what is war and what is not, predicated on wholesale death and destruction may no longer hold true for an increasing number of conflicts. And while the DoD has certainly made some organizational changes to adapt, and have likewise acknowledged the threat, I believe it has not yet grasped the extent of that threat and as such, has not made the necessary organizational changes. Our adversaries are thinking *asymmetrically* because *we have forced them to think--and act--asymmetrically*--they simply cannot "take us on" symmetrically. Yet there will always be conflict given the necessity to constantly maintain the balance of power in an anarchistic international security environment, leaving our adversaries no other choice with which to realize *their* national security objectives.

It is with the past history afforded us through the intent of the *Kriegsakademie* and the original conception of ACTS, together with ACSC's fundamental purpose, that this paper considers this fundamental question: "Does the past embodiment, current instantiation and continued acceleration of the weaponization of information support its emergence as a separate service, co-equal with its five sister services, and if so, what elements from those services should be incorporated into a single service construct?"

Before we begin to take advantage of the opportunity afforded by PME, I would like to first thank several people. First, I would like to thank PA Denk and Dr. Froelich from the Maxwell Clinic for correctly diagnosing and treating me with compassion and respect after I fractured my lower vertebrae. They truly represent what all Air Force Medial Staff should strive to be. I would also like to thank Maj Greg Durand for his friendship, sense of humor and help. Likewise, I would like to thank Maj Greg Reiter and his wife Audrey for their compassion, friendship, and hospitality. Several faculty members were critical to this project as well. Dr. Paul Kan and LtCol Reynolds encouraged me to think innovatively, supported and focused my undisciplined thoughts, and opened my eyes to the more profound world of International Relations, which I hope to pursue further. I would like to thank both LtCol Ide, LtCol Jim Jovene and Majs Jeffery "Can" Scott, Scott "Sleepy" Schlieper and Kurt "Coyote" Austin for their support after my injury, and never making me feel less of a contributor when I could not always participate. I would like to thank my faculty advisors, Maj Tom "Chill" Childress and Maj Bridget Carr for their sincerity, remarkable encouragement, support when source material was difficult to liberate, and incredible patience for this project. Finally, none of this would have been possible without my wife Kim's inhuman patience, frequent flights, constant encouragement and unconditional love and support.

Notes

[1] Honorable Newt Gingrich, "Commandant's Speakers Series (CC-812)," lecture, Air Command and Staff College, Maxwell AFB, AL, 6 March 2002.

[2] Dr. Richard Paul and Dr. Linda Elder. *The Miniature Guide to Critical Thinking: Concepts and Tools*. Rohnert Park, CA: Foundation of Critical Thinking, 2000, 1-2.

[3] "One gained entrance to the *Kriegsakademie* only by passing a rigorous examination that lasted sixteen hours, and only a small percentage of the officer corps was able to pass that hurdle." (See: Murray, Williamson Dr., Lindbergh Professor, National Air and Space Museum. Address. Naval Post Graduate School and Office of Naval Research Conference on Military Education for the 21st Century Warrior, Monterey, CA, 15 January 1998.)

[4] "War Theory Reflection Questions." *Air Command and Staff College Distance Learning Program*. Lesson TH505. ACSC Multimedia Edited Version 2.2. CD-ROM. August 1997, n.p.

[5] Christopher R. Gabel. "The Leavenworth Staff College: A Historical Overview." *Military Review*, Sep-Oct 1997, n.p. On-line. Internet, 15 February 2002. Available from http://www-cgsc.army.mil/milrev/english/sepoct97/almanac.htm.

Notes

[6] "War Theory Reflection Questions."

[7] Muller, Dr. Richard R. "The Luftwaffe and Barbarossa, 1941." In *Airpower Studies: AP Coursebook Academic year 2002*. Compiled by LtCol Micheal Fiedler, Phd, et al. Air Command and Staff College: Department of International Security and Military Studies. Maxwell, AFB, AL: Air University Press, August 2001, 212.

[8] "Fort Leavenworth's first Army school was the School of Application for Infantry and Cavalry. [It opened in 1882.] From 1904 to 1917, GSSC included two separate courses: the School of the Line and the Army Staff College that, together, prepared officers for staff duties at division, corps and general staff levels. In 1922, the School of the Line and the Staff College merged to form the Command and General Staff School (CGSS). The early Leavenworth college (USCG) borrowed heavily from the Kriegsakademie in terms of curricula and methodology." (See: Gabel, Christopher R. "The Leavenworth Staff College: A Historical Overview.")

[9] Gabel, "The Leavenworth Staff College: A Historical Overview."

[10] US Department of Defense. *Quadrennial Defense Review Report*. Washington DC: U.S. Government Printing Office, Sep 2001, iii.

[11] Major Dwight H. Griffin, et al. "The Air Corps Tactical School: The Untold Story." *Air Command and Staff College Distance Learning Program*. Lesson TH508. ACSC Multimedia Edited Version 2.2. CD-ROM. August 1997, 4.

[12] Ibid.

[13] Sun Tzu. *The Art of War*. Edited and translated by Samuel B. Griffith. (New York: Oxford University Press: 1971), forward.

[14] Ibid.

[15] Toby Harnden. "Rumsfeld Calls For End To Old Tactics Of War." London Daily Telegraph, 16 October 2001.

[16] This is the fundamental tenet of Clausewitz's principle of duality where he noted: "[I]f we are really waging war, we must return the enemy's blows; and these offensive acts in a defensive war come under the heading of the 'defense'--in other words, our offensive takes place within our position or theater of operations. Thus a defensive campaign can be fought with offensive battles, and in a defensive battle, we can employ our divisions offensively. Even in a defensive position awaiting the enemy assault, our bullets take the offensive. So the defensive form of war is not a simple shield, but a shield made up of well directed blows." This was demonstrated in the Arab-Israeli Six-day war, where Israel was forced into offensive means to prevent attack. (See: Carl von Clausewitz. *On War*. Edited and translated by Michael Howard and Peter Paret. (Princeton NJ: Princeton University Press, 1976), 357.)

[17] "Mission Needs Analysis (MNA). An analysis designed to assess one's ability to accomplish the tasks identified during the Mission Area Analysis. The [MNA] uses a task-to-need methodology to identify mission needs. It can also highlight technological opportunities and identify reliability and maintainability improvements that enhance warfighting capability." (See: CJCS 3170.01B. *Requirements Generation System*, 15 Apr 2001, C-A-1.

[18] Simplicity, Unity of Effort, Mass, Maneuver, Objective, Offensive, Surprise, Economy of Force, and Security. (See Appendix A.)

Notes

[19] LtCol Joe Reynolds. “How to Study Things . . . Like Airpower.” *Airpower Studies AP Coursebook Academic Year 2002*. Air Command and Staff College Department of International Security and Military Studies. Aug 2001, 4.

Abstract

Information Superiority is an overarching and integrating construct in both Joint Vision 2020 and the 2001 Quadrennial Defense Review and is codified in both the 2000 National Security Strategy (NSS) and the 1997 National Military Strategy (NMS) . Yet the services still have no comprehensive definition of information operations (which provides for information superiority) and in fact, offer transposed definitions of Information Warfare (IW), Information Operations (IO), and Command and Control Warfare (C2W). This confusion precludes effective development of doctrine, training and unity of effort. This paper uses the objective construct of a Mission Needs Statement to discipline the following question: "Does the past embodiment, current instantiation and continued acceleration of the weaponization of information support its emergence as a separate service, co-equal with its sister services, and if so, what elements from those services should be incorporated into a single service construct?"

Its main goal is to offer an alternative construct to the historical Western prescription of kinetic, force-on-force enemy contact, inculcated in American doctrine and culture, to best prepare for both the ongoing conflict and the next war. It highlights the concern that even as the DoD--and American society--become more dependent on information, they become more vulnerable as a result of that dependency. Yet there is no proportionate increase in defensive measures or the necessary organizational transformation to strengthen those defenses. The research concludes that a separate service can best focus limited resources and provide true systems-of-systems (SoS) engineering, developed *a priori* as proper architectural constructs, and will best meet the economic, military, and political needs of a future multi-dimensional war. It will show a separate service will likewise best support national security objectives by exploiting the inherent synergy between C4ISR, information operations, information-in-warfare, space operations, and electronic warfare. The research concludes by offering a strawman construct on the structure of such an Information Service.

Chapter 1

Introduction

> *The QDR highlights both the imperative for the United States to maintain an unsurpassed capability to conduct information operations, as well as the need to strengthen U.S. capabilities in these areas. DoD must also develop an integrated approach to developing information system requirements, acquiring systems, and programming for the force of tomorrow. The ability to conduct information operations has become a core competency for the Department.*
>
> —2001 Quadrennial Defense Review

This chapter introduces the problem, the framework and the strategy to attack the question posed in the abstract. The problem is determining the viability of creating a separate Information Service (I-Service) to meet the QDR vision with respect to Information Operations (IO). The scope and potential for parochialism demand the strategy for analyzing that problem be objective, logical, and precedented. The DoD acquisition system provides such a framework through CJCS 3170.01B and the DoDD "5000" acquisition series, which together discipline all DoD acquisitions. All major DoD acquisitions begin with a Mission Needs Statement (MNS), "a non-system-specific statement of operational capability need written in broad operational terms."[20] The MNS documents the results of a Mission Needs Analysis (MNA) which determines if the extent of a new threat requires no change, changes to an existing system, or development of a new system. Thus, the strategy employed analogizes a new service as a new system acquisition and then uses the common vernacular, familiar construct, and proven objectivity of the MNS structure to adjudicate the need for that new system. A MNS meets stringent, inflexible criteria:

1. Identify the connection to the Defense Planning Guidance (including connection to the NSS and QDR)[21]
2. Identify the nature of the threat and the need to counter that threat[22]
3. Identify *non-materiel* alternatives (i.e. explain why current systems cannot meet the threat)[23]
4. Identify potential *materiel* alternatives (i.e. explain the construct of new system)[24]
5. Identify constraints (explain manpower, facility, legal, etc. constraints)[25]

Additionally, the MNS construct ties the I-Service structure to a *capability-based* architecture,[26] (a critical evolution for the Administration), against a non-specific threat vice instantiated nation-state threats. The caution here is that threats--not capability--still drive the DoD budget (Fig. 1). 1. Table 1 organizes the resulting framework.

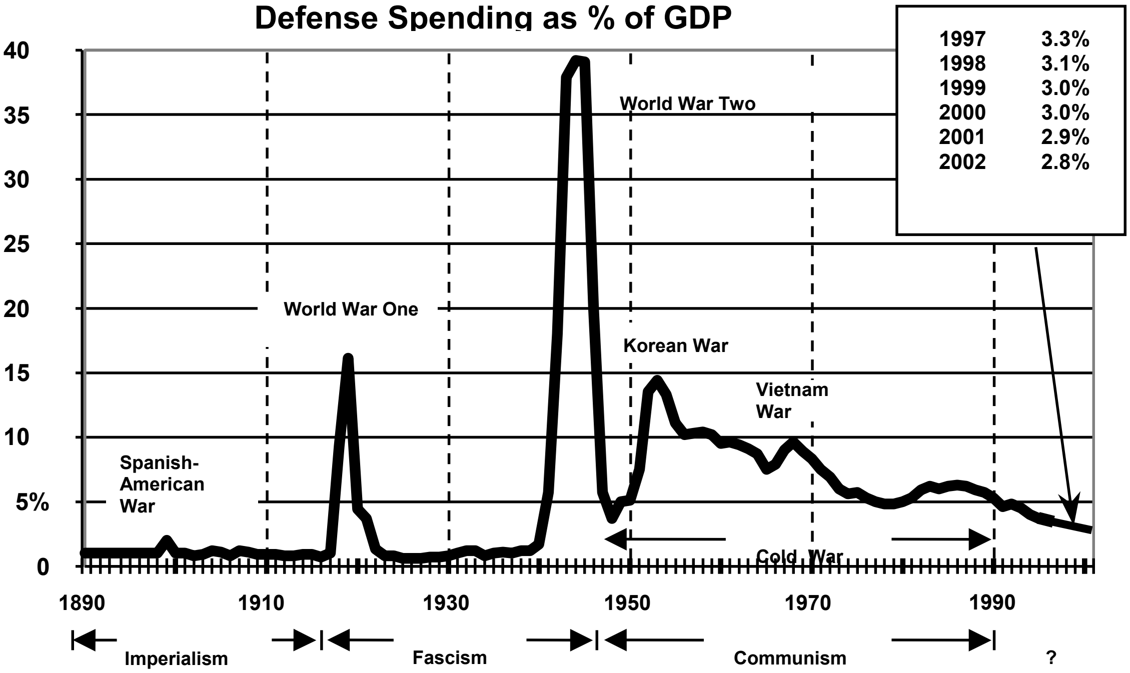


Figure 1: Defense Spending As Function of Threat[27]

Table 1: Research Organization Based on MNS Structure

MNS Criteria	Research Equivalent	Chapter/Appendix	Main Conclusions
N/A	Overview	1 Introduction	- The framework is logical and objective
1. Identify the connection to the Defense Planning Guidance	Is there a threat established in the NSS, NMS, and QDR? *If so . . .*	- Preface - Pervasive--used to initiate, and used throughout, each chapter	- All conclusions centered on QDR's six main goals
2a. Identify the nature of the threat	Is that threat broad and enduring? *If so . . .*	2 The Threat	- The threat is broad and enduring with respect to time, the continuum of actors, the conflict spectrum and the IOPs
2b. Identify the Need	What is the scope of the countermeasure to neutralize that threat now and in the future? *If so . . .*	3 The Need for a Countermeasure	- The DoD needs standardized definitions of IO and the Infosphere and a single IO Lead - C4ISR, EW, and space operations are symbiotic and should be treated as a single mission area
3. Identify Non-material alternatives	Does that countermeasure require a separate service to be effective? *If so . . .*	4 The Status Quo	- "The requirements for that unique expertise are not being fulfilled"[28] - "The resources of that expertise are not being used properly"[29] - "Only an independent [Service] can provide a capability that is considered vital to national defense."[30] - The I-Service meets the same criteria as do the other services
4. Identify Potential Material Alternatives	What would be the main components of that service?	5 The Information Service	The I-Service would - Consist of a small cadre of military - Be supported largely by industry - Have a similar structure to that of the Coast Guard to optimize the civilian-military duality of its mission while preserving Posse Comitatus
5. Constraints	Not included due to space limitations	- Pros/Cons included throughout report	- Main constraints: -- Perceived Cost -- Personnel -- Inertia -- Space Command -- Services concern with potential non-support

Chapter 2 proves the threat is broad and enduring with respect to time, the continuum of actors, the conflict spectrum, and the national scope. Chapter 3 details the scope of the countermeasure needed to neutralize that threat now and in the future. It postulates a unifying definition to best focus limited resources. Chapter 4 proves that the current DoD structure (i.e. the non-materiel solution) has proven itself sub-optimal in defending against the threat by proving several primary and secondary assertions with respect to the problem, based primarily on span of control, dogmatic thinking, and incompatibilities with the current military establishment. Chapter 5 provides a strawman of the materiel alternative--i.e. the I-Service. It defends the premise that a military vice a civilian agency is required, and should be supported by an industrial base that has already far surpassed the military in terms of Information Technology (IT). Appendix A provides a summarized list of near-term actions to eventually enable an I-Service. Chapter details are included in subsequent, respective appendices--i.e. Appendix *B* provides details corresponding to Chapter *2*, Appendix *C* corresponds to Chapter *3*, etc.

Notes

[20] CJCS 3170.01B. *Requirements Generation System*, 15 Apr 2001, C-A-1. Note: "MNS" is pronounced "mins."

[21] "Defense Planning Guidance Element. Identify the major program planning objective or section of the Defense Planning Guidance to which this need responds. Also reference the Joint Intelligence Guidance, DOD Strategic Plan (Quadrennial Defense Review), and Military Department long-range investment plans, if applicable." (See: CJCS 3170.01B. *Requirements Generation System*, 15 Apr 2001, C-A-1.)

[22] "Mission and Threat Analyses. Discuss the Defense Intelligence Agency-validated threat to be countered as well as the projected threat environment and the shortfalls of existing capabilities or systems in meeting these threats. Comment on the timing of the need and the general priority of this need relative to others in this mission area." (See: CJCS 3170.01B. *Requirements Generation System*, 15 Apr 2001, C-A-1.)

[23] "Nonmateriel Alternatives. Discuss the results of the mission needs analysis. Identify any changes in US or allied doctrine, operational concepts, tactics, organization, and training that were considered in the context of satisfying the deficiency. Describe why

Notes

such changes were judged to be inadequate." (See: CJCS 3170.01B. *Requirements Generation System*, 15 Apr 2001, C-A-1.)

[24] "Potential Materiel Alternatives. Identify known systems or programs addressing similar needs that are deployed or are in development or production by any of the Services, agencies, or allied nations. Discuss the potential for inter-Service or allied cooperation. Indicate potential areas of study for concept exploration, including the use of existing US or allied military or commercial systems, including modified commercial systems or product improvements of existing systems." (See: CJCS 3170.01B. *Requirements Generation System*, 15 Apr 2001, C-A-1.)

[25] "Constraints. Describe, as applicable, key boundary conditions related to infrastructure support that may impact on satisfying the need: available facilities; logistics support; transportation; global geospatial information and services support; manpower, personnel, training, environmental, and occupational health constraints; spectrum supportability; command, control, communications, and intelligence interfaces; security; standardization and interoperability within DOD components, North Atlantic Treaty Organization, other allies and friendly nations, as well as US Government agencies and non-Government organizations. Address the operational environments (including conventional; initial nuclear weapon effects; nuclear, biological, and chemical contamination; electronic, electromagnetic and natural) in which the mission is expected to be accomplished. Define the level of desired mission capability in these environments." (See: CJCS 3170.01B. *Requirements Generation System*, 15 Apr 2001, C-A-2.)

[26] "The new defense strategy is built around the concept of shifting to a 'capabilities-based' approach to defense. . . . A capabilities-based model--one that focuses more on how an adversary might fight than who the adversary might be and where a war might occur--broadens the strategic perspective. It requires identifying capabilities that U.S. military forces will need to deter and defeat adversaries who will rely on surprise, deception, and asymmetric warfare to achieve their objectives." (See: US Department of Defense. *Quadrennial Defense Review Report*. Washington DC: U.S. Government Printing Office, Sep 2001, 14)

[27] Loren B. Thompson. Phd. *Rumsfeld's Challenge: Does this Ship Turn.* Briefing. Lexington, MA: Lexington Institute, August 2001, 4.

[28] Shawn P. Rife. "On Space Power Separatism." In *Airpower Studies: AP Coursebook Academic Year 2002*. Compiled by LtCol Micheal Fiedler, Phd, et al. Air Command and Staff College: Department of International Security and Military Studies. Maxwell, AFB, AL. Aug 2001, 393.

[29] Ibid.

[30] Ibid.

Chapter 2

Mission Threat Analysis: The Threat

> *Technological advances create the potential that competitions will develop in space and cyberspace. Space and information operations have become the backbone of networked, highly distributed commercial civilian and military capabilities. Similarly, states will likely develop offensive information operations and be compelled to devote resources to protecting critical information infrastructure from disruption, either physically or through cyber space.*
>
> —2001 Quadrennial Defense Review

> *Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in nontraditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and nontraditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.*
>
> —Presidential Decision Directive 63

Section II of an MNS details the significance of a new or evolved threat based on government policy and independent threat analyses to ascertain its nature, scope, and extent. This chapter show the IO threat is both broad and enduring with respect to time, the continuum of actors, the conflict spectrum, and underpins all national IOPs (Fig. 2). It also demonstrates that *threat* is growing even as US *vulnerabilities* are growing.

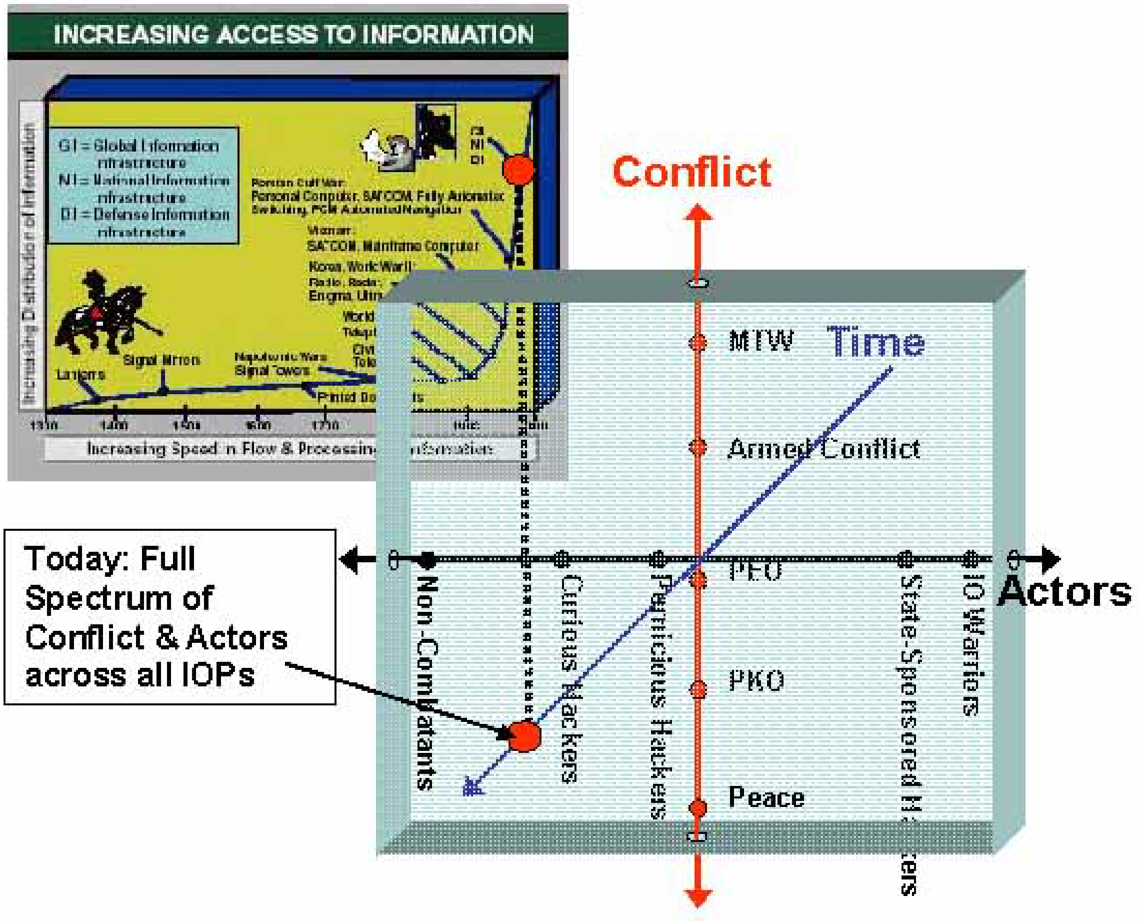

INCREASING ACCESS TO INFORMATION
GI = Global Information Infrastructure
NI = National Information Infrastructure
DI = Defense Information Infrastructure
Persian Gulf War: Personal Computer, SATCOM, Fully Automatic Switching, PGM Automated Navigation
Vietnam: SATCOM, Mainframe Computer
Korea, World War II: Radio, Radar, Enigma, Ultra
World
Civil
Signal Mirrors
Lanterns
Napoleonic Wars Signal Towers
Printed Documents
GI
NI
DI
1300
1400
1500
1600
1700
1900
Increasing Distribution of Information
Increasing Speed in Flow & Processing Information
Conflict
MTW
Time
Armed Conflict
PEO
PKO
Peace
Actors
Non Combatants
Curious Hackers
Pernicious Hackers
State-Sponsored Hackers
IO Warriors
Today: Full Spectrum of Conflict & Actors across all IOPs

Figure 2: Information Window With Respect To Actors/Time/Conflict Spectrum[31]

<u>The threat is broad and enduring with respect to time.</u> "All warfare is based on deception."[32] And all deception is based on information whether one simply denies it from an adversary, alters it in a such a way that the adversary is maneuvered into a desired course of action (COA), or uses it to overwhelm the adversary's Observe-Orient-Decide-Act (OODA) Loop. Information--and denying it--has been central to conflict since primitive tribes first fought over resources. Couriers (i.e. early communication systems) became so critical as Total War emerged during the Napoleonic era, they were protected under the law of warfare and could not be harmed.[33] Information will remain critical as it is the essential element behind the balance of power, necessitated by the current international system of structural realism. States learn what an adversary, ally, or competitor is doing that could affect its own national security, and act to mitigate any advantage.[34]

All the venerable military strategists recognized the criticality of information as well. Sun Tzu and Niccolo Machiavelli[35] were but two of the many strategists who recognized information could actually *preclude* war by decimating the enemy's plans without armed force, with the latter noting: ". . .to subjugate the enemy's army without doing battle is the highest of excellence. Therefore, the best warfare strategy is to attack the enemy's plans, next is to attack alliances, next is to attack the army, . . . "[36] Modern strategists agree. Liddell Hart noted "[t]he real target in war is the mind of the enemy commander, not the bodies of his troops."[37] Clausewitz elevated information to the **same level** of the fundamental construct of war--danger, direct force, and friction--devoting an entire chapter of *On War* to the subject noting information was "the foundation of all our ideas and actions."[38] Jomini demanded his generals neglect no opportunity to gather information.[39] Finally, AF doctrine states: "Dominating the information spectrum is as critical to conflict now as controlling air and space, or as occupying land was in the past."[40]

The threat is broad and enduring with respect to the Set of Actors. Information is not only critical to military operations, but to every aspect of modern life. Yet it can be exploited and denied by a broad range of actors ranging from state actors, to state-sponsored actors, to non-state actors (e.g. hackers). Examples follow:

State Actors. The QDR supports the assertion that the next peer competitor appears to be China or a resurgent Russia in the next 15-20, stating:

"Asia is gradually emerging as a region susceptible to large-scale military competition. Along a broad arc of instability that stretches from the Middle East to Northeast Asia, the region contains a volatile mix of rising and declining regional powers."[41]

The Chinese continue a robust and pervasive restructuring of their armed forces begun in the early 1990's into a lighter, more expeditionary force. They are also "working to incorporate the concepts of modern warfare …and have placed a priority on developing the technologies and tactics necessary to conduct rapid tempo, [high-tech] warfare."[42] This is in line with the Asian Way of Warfare as well. Maoist in theory, it is the type of war China would have to fight against a technologically superior foe, like a US-led coalition. US dependence on Information "places a bull's eye on C4ISR."[43] Dr. Paul Kan, an instructor at ACSC specializing in International Relations with a concentration in Asian/Pacific Security, explains the Asian view of war as being centered around vulnerabilities and strengths--using one's strengths against an adversary's vulnerabilities.[44] Yet the DoD remains structured symmetrically,[45] and geographically. Even a future peer competitor will not likely try to engage the US directly, given the overwhelming force in a direct force-on-force engagement.[46] Several independent analyses support Dr. Kan's conviction. The U.S. Report on China's Military Power states "China increasingly is viewing [IO/IW] as a strategic weapon to use outside of traditional operational boundaries."[47] Synthesizing these independent analyses in tabular form (Table 2) highlights the evident focus of Chinese preparation:

Table 2: Focus of Chinese Military Evolution

Asymmetric		Symmetric	
General	**IO/C4ISR/EW-Specific**	**General**	**IO/C4ISR/EW-Specific**
- A preponderance of thought on **fighting without winning**, particularly through preemptive attacks that turn American public against any effort[48]	- Importing "a variety of foreign technologies," and technical assistance which could be used to develop ground-based anti-satellite (ASAT) capability including lasing and optical ranging systems."[49]	- Continued reliance on hardened command complexes remaining from the build-up against Russia and impervious to all but the most lethal US PGMs	- Increased emphasis on EW, mainly through reverse engineering Western products[50]
- A strategy of "victory through inferiority over superiority."[51]	- Developing GPS jammers[52]	- An aggressive program to procure modern SAM systems[53]	- Accelerated and aggressive development of electronic countermeasures (ECM) doctrine, including subsequent training[54]
- Continued aggressive C4I. Because "China still lags far behind western standards for controlling complex joint operations and lacks the robust C4I architecture required to meet the demands of the modern battlefield" preemptive, asymmetric attacks are expected[55]	- China's military-backed industries also have entered into joint ventures with foreign firms to produce GPS receivers, which may find their way to military weapons."[56]	- A highly redundant C3 structure **separate from the more vulnerable** civilian PSTN network providing for multiple redundancies[57]	- Stealth technology/warfare including aircraft, ships, tanks, and missiles noting. "In future wars . . .target detection will mean immediate elimination"[58]
Continued exploitation of the civilian cell phone market[59]	- Accelerated development of methods for computer network attack (CNA)--as part of its overall IO strategy. The report concluded that "as it develops more expertise in defending its own networks against enemy attack, it is likely to step up attempts to penetrate foreign information systems."[60]	- Precision warfare: . . .precision in reconnaissance (spying) and advance warning, in information transmission, in command coordination, in mobile positioning, in target strikes, and in [BDA].[61]	- China is believed to have a highly developed electro-optic industry, as well as the ability to field blinding laser weapons, including tactical laser weapons[62]
- Veiled peacetime demands for virus samples and antidotes as a predicate for doing business with US software firms[63]	- "Computer virus warfare. In future wars, operations against military computers will become a key type of information warfare."[64]	- Rapidly take the offensive. They noted that "Yugoslav and Iraqi forces were defeated due to excessive passivity" and that both Saddam and the Serbian army should have taken offensively attack the. US infrastructure[65]	- "China will purchase a new generation of high-tech military equipment from Russia worth $15B and cooperate with Russia in producing 180 to 200 Su-27 modified fighters."[66]

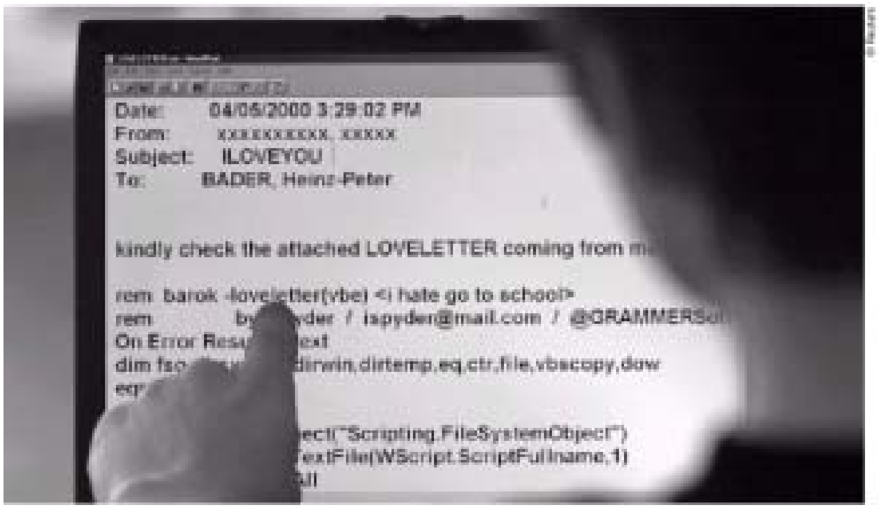
Table 2 (Cont.): Focus of Chinese Military Evolution

Asymmetric		Symmetric	
General	**IO/C4ISR/EW-Specific**	**General**	**IO/C4ISR/EW-Specific**
	- China and Russia will cooperate in developing a new generation of military aircraft and surface-to-surface, surface-to-air and air-to-air missiles; in developing laser, light-beam, neutron and other high-tech weapons; and in conducting joint military exercises and live, simulated hi-tech maneuvers.[67]	- Launch pre-emptive attacks[68] before the enemy (the US -led coalition) can assemble its forces, particularly when they are in political deliberations to counter the US's publicly announced JV2020 approach--rapid, full spectrum[69]	- China and Russia have teamed to develop a joint countermeasure against a US ABM system[70]
		Priority on strategies that will rapidly lead to domination of "land, air, sea, space, and electromagnetic spheres of the battlespace"[71]	

Sources: Multiple.

It is even more instructive to analyze what the Chinese are not investing in. There is no evidence China is currently developing either the capability to conduct launch-on-demand launch operations or a global satellite tracking network.[72] The implication is clear: with their emphasis in EW, space control, laser development, and an operational model far less dependent on space, they appear to be planning to attack US space systems with ground-based jammers deep inside China where US forces cannot negate them without violating Chinese airspace. The Chinese can then hold US space systems hostage for political gain, no different than when they held the EP-3E crew in April 2001.[73]

Non-State Actors. The economy of the U.S. and indeed the world depends on electronic networks--millions of messages and billions of dollars are transferred over them daily. The Defense Science Board (DSB) agrees--noting "the threat . . . goes well beyond the [DoD] . Every aspect of modern life is tied to a computer system at some

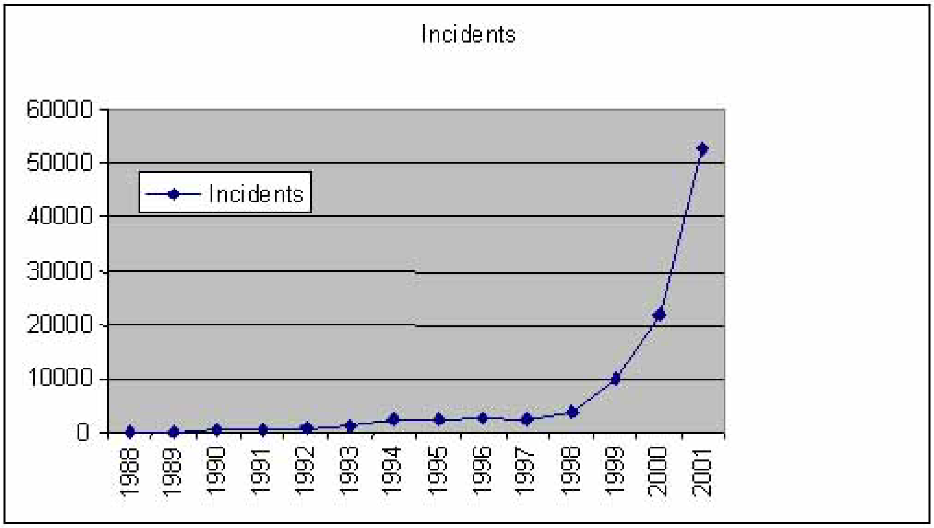


```
Date:      04/06/2000 3:29:02 PM
From:       xxxxxxxxxx, xxxxx
Subject:    ILOVEYOU
To:        BADER, Heinz-Peter

kindly check the attached LOVELETTER coming from m

rem  barok -loveletter(vbe) <i hate go to school>
rem            by     yder / ispyder@mail.com / @GRAMMERS
On Error Res      ext
dim fs             dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq

                ect("Scripting.FileSystemObject")
                extFile(WScript.ScriptFullname,1)
                ll
```

Figure 3: Non-State Actors . . . Or Not?[74]

point, and most of these systems are relatively unprotected."[75] Independent and state-sponsored hackers have proven this vulnerability time and time again and as such, their appeal as targets. Table 3 summarizes some of the more costly cyberattacks, estimated to represent only 7-20% of the actual number.[76] Of particular concern is the secondary effects computer network attacks (CNA) could have. Lacking signals intelligence assets, a third world power could launch a computer attack in order to *maneuver* the DoD to means that can be compromised. For example, in the Code Red attack, the DoD took many networks off-line and instead "[tried] to determine other ways of allowing the public to access information -- telephones, fax machines, or other ways of communication."[77]

Cyberattacks are deceptive. They are nearly impossible to trace and few leave audit trails. The DSB emphasized "a structured [IO] attack could be [executed] by a foreign country or terrorist group under the guise of unstructured hacker-like activity and, thus, could cripple U.S. readiness and military effectiveness."[78] CNA is therefore a superior form of asymmetric warfare--inexpensive IO methods to persistently wear down the economic backbone of a country, while [simultaneously] devastating its infrastructure.[79]



And there are far more people, creating far more vicious attacks (Fig. 4) than ever before, as software becomes more complex and subsequently more vulnerable. Tools, as shown in Fig. 5, likewise are becoming far more available and far more destructive, for

Figure 4: Information Attacks Are Increasing at an Exponential Rate

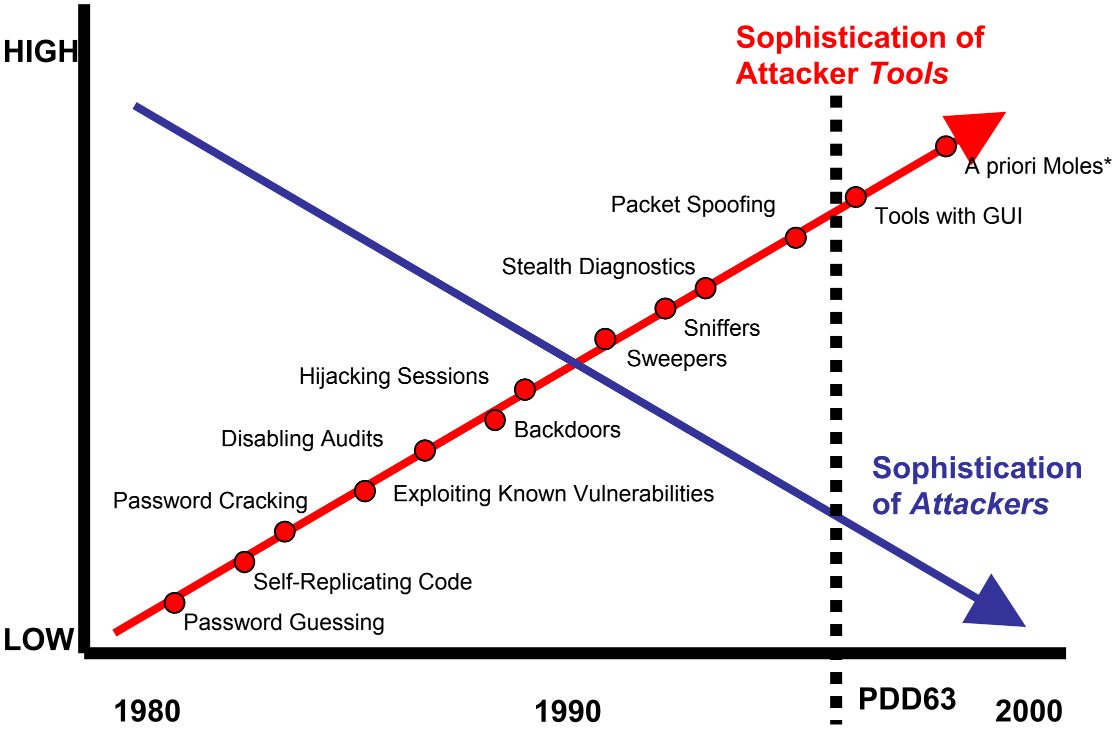


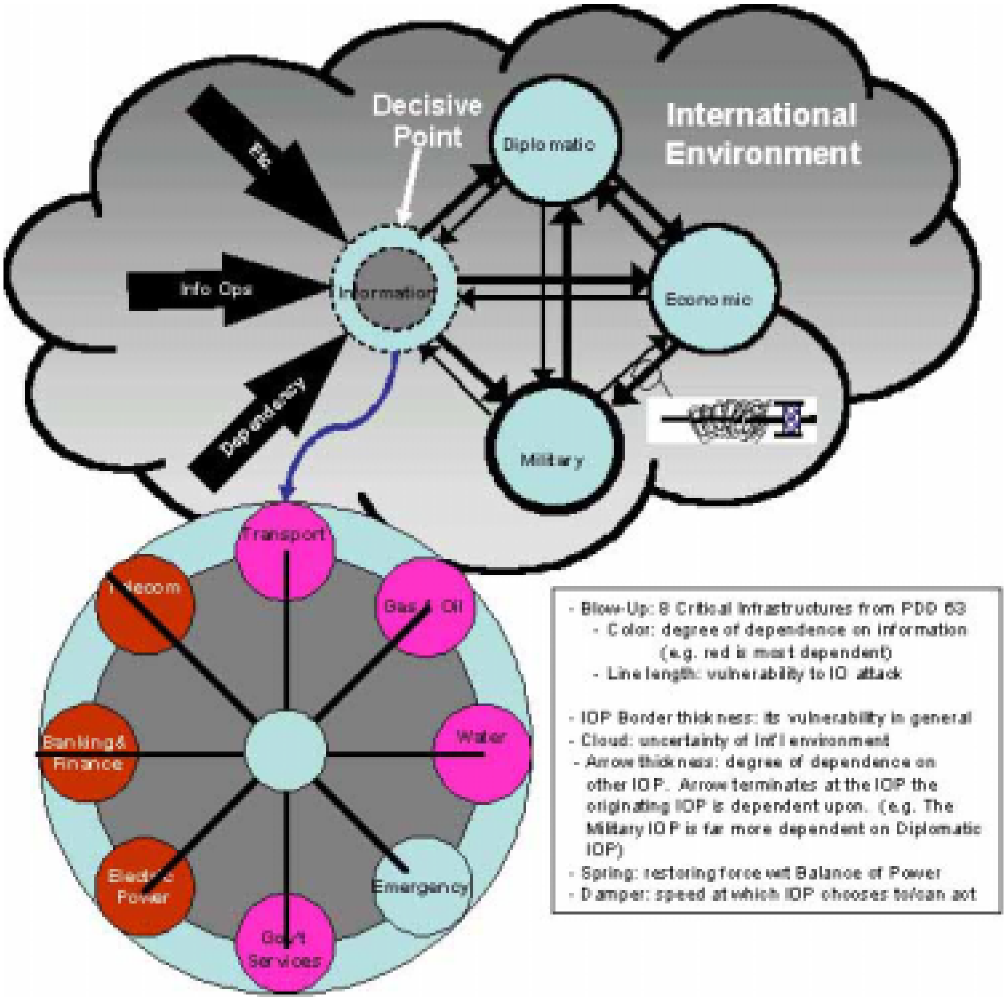
Figure 5: Trends in Cyberwarfare[80]

non-political purposes. Being non-political, such acts do not meet the criteria of war, i.e. “organized violence carried on by political units against each other,” further perplexing the military mindset on what constitutes a legal combatant or even a traitor. [81]

Table 3: Cyberwarfare Damage

Year	Code Name	Actor	Worldwide Economic Impact (‘01, US $B)	Payload[82]	# Computers Affected (M)	Affected
2001	Nimda	Hacker	$0.635	- Worm: Non-destructive - Compromised the security of infected hosts - Acting as SoS - Indiscreet Subject Line[83]	8.3	
2001	Code Red(s)	Hacker	$2.62	- Worm: Installed “back doors" on infected computers, leaving them vulnerable to future hacking[84]		- Qwest Comm - Microsoft - AT&T - FedEx[85]
2000	Love Bug	Hacker	$8.75	Virus: Destroyed Data	45	- Silicon Graphics - DoD - Federal Reserve - Others86
1999	Melissa	Hacker	$1.10	- Macro Virus - Precursor agent - Lowered security settings on MS computers making them vulnerable to other viruses		
Ongoing	Moonlight Maze	State-Sponsored (Russia)	- Significant data threat at the unclassified and classified levels	- Distributed coordinated attacks	DoD and University networks	Data Theft -“naval codes and data pertaining to missile guidance systems.”[87]
30 Apr to 6 May 2001	May Day	State-Sponsored (China)	Minor	- Data degradation and alteration	DoD and University networks	- Hacked and defaced sites

Source**:** Multiple.



- Blow-Up: 8 Critical Infrastructures from PDD 63
  - Color: degree of dependence on information (e.g. red is most dependent)
  - Line length: vulnerability to IO attack
- IOP Border thickness: its vulnerability in general
- Cloud: uncertainty of Int'l environment
- Arrow thickness: degree of dependence on other IOP. Arrow terminates at the IOP the originating IOP is dependent upon. (e.g. The Military IOP is far more dependent on Diplomatic IOP)
- Spring: restoring force wrt Balance of Power
- Damper: speed at which IOP chooses to/can act

Figure 6: Information IOP As Decisive Point[88]

__**The threat is broad and enduring with respect to IOPs.**__ All Instruments of Power (IOP) are critical to the national security structure, ensuring strategic security goals can be achieved and sovereignty remain unchallenged. The NSS states:

> "An extraordinarily sophisticated information technology (IT) infrastructure fuels America's economy and national security. Critical infrastructures, including telecommunications, energy, finance, transportation, water, and emergency services[89], form a bedrock upon which the success of all our endeavors--economic, social, and military--depend. These infrastructures are highly interconnected, both physically and by the manner in which they rely upon [IT] and the national information infrastructure."[90]

While no one IOP operates in a vacuum (Fig. 6), Information increasingly underpins the other three, yet has proven to be the most vulnerable, even as US society becomes more dependent on it in peace, conflict, and war. To attack these **centers of gravity,**[91] an adversary will use the weakest **decisive point**, which this chapter has shown to be the Information IOP.[92] In addition, the other IOPs benefit from Unity of Effort--Constitutional balances of power ensure the Diplomatic and Military IOPs exercised by the President in concert with Congress are focused, while the Economic IOP achieves Unity of Action through international market controls and an international body of law. The Information IOP however, is rudderless, lacking both Unity of Action and Unity of Command.

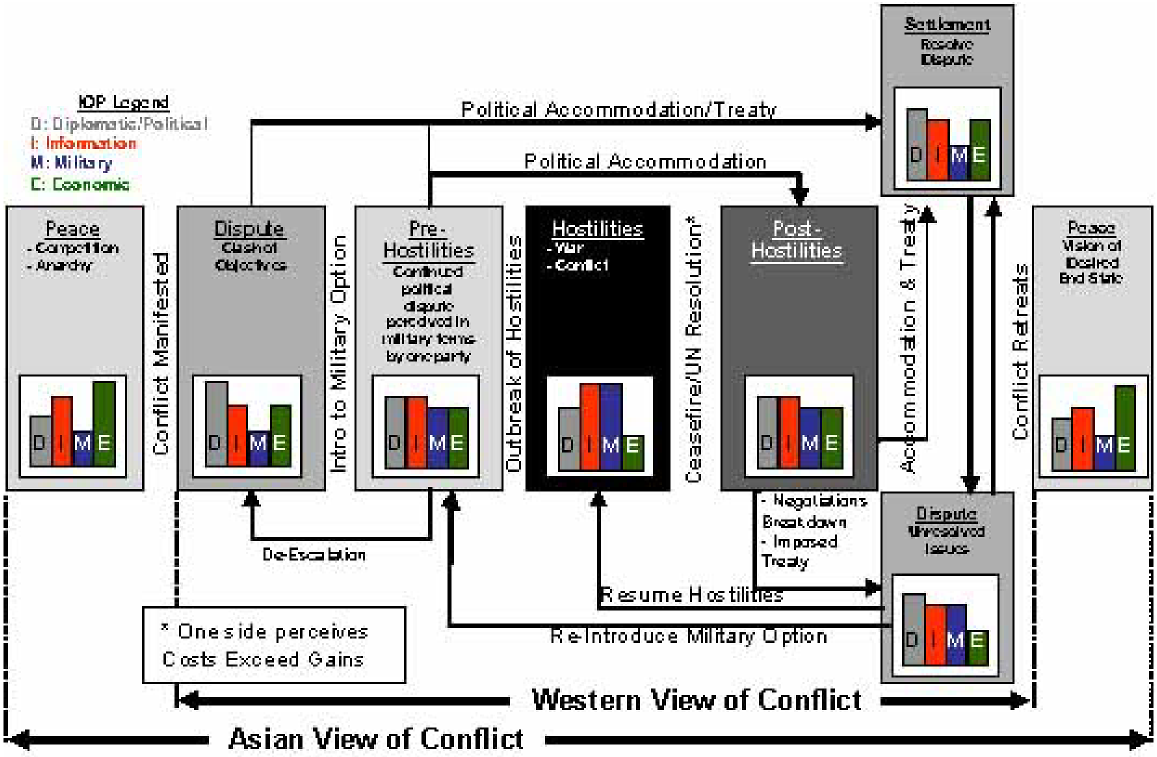


Figure 7: IOPs in the Conflict Spectrum[93]

That U.S. infrastructure will increasingly be accessible and managed through the Internet, making it particularly vulnerable.[94] Tom Ridge, the director of the Office of Homeland Security "hammered home" the pervasive nature of IT, warning "[d]estroy the networks and you shut down America."[95] Two significant sources of concern are the Y2K fixes and the telecommunications infrastructure, the latter due to the sheer amount of Y2K fixes outsourced to foreign countries, offering myriad opportunities to install covert backdoors.[96] The civilian (and therefore DoD) telecommunications infrastructure too is a particular concern. In May 1998, 40M people were left without pager, ATM, and/or cell-phone service when a *single* communications satellite, *Galaxy IV,* permanently failed with no back-up.

That civilian telecommunications infrastructure is critical to the DoD as well, in that 95% of all military communications is routed through commercial lines, including highly sensitive intelligence data, which while not decipherable, remains highly vulnerable to jamming.[97] (That infrastructure is becoming increasingly dependent on GPS as well, in that the precision timing provided by GPS synchronizes many of the internet and cellular protocols, and is likewise highly susceptible to jamming.[98]) Capt DelVecchio researched the vulnerability of these DoD phone networks in that so many DoD phone calls travel trough international switches.[99] His research found critical dependencies and security concerns making DoD links, including secure DSN links, highly susceptible to tampering, re-routing, and monitoring by any adversary--military or economic,[100] making it a concern at every level of the conflict spectrum.

The threat is broad and enduring with respect to the spectrum of conflict. With respect to Fig. 7, note that Information has matured into a *force application* role.[101] IO weapons have been used by non-state actors, US Armed Forces, and adversaries against the U.S. In **Operation Enduring Freedom (OEF)**, the US used its diplomatic IOP to shut down Somalia's government, economy, and civilian infrastructure when it convinced AT&T and British Telecom to cut off Somalia's only international gateway, blocking Al

Qaeda financial transactions. In **Operation Restore Democracy (ORD)**, a Peacekeeping *Humanitarian* Action in Haiti, a number of technical IO weapons were developed to shut down the water and electricity, immobilize gas pumps, and "[jam] local radio and television stations."[102] In **Operation Deliberate Force (ODF)**, a Peace *Enforcement* action, the DoD conducted computer attacks against the Yugoslavian IADS network. Finally, Desert Storm, a Major Theater War, "leveraged information [and] brought to warfare a degree of flexibility, synchronization, speed and precision heretofore unknown. By exploiting knowledge, it devastated Iraq's formidable military machine"--and showed the world what to expect, and how to prepare.[103] Information dominance has always been a critical factor in war, as described in the first part of this chapter, but "STORM was different. . .it was a war where an ounce of silicon in a computer may have had more effect than a ton of depleted uranium."[104]

Summary. This chapter proved the threat is broad with respect to the conflict spectrum, actors, IOPs and time. The threat is growing because the need for information is growing. But even as information becomes more critical, its development and exploitation continues to fracture among the services and even ten years after the first information war, the DoD has not yet standardized definitions, doctrine, or organizational focus. Many high-ranking officials,[105] as well as the Chinese, have warned of a coming *Electronic Pearl Harbor*. The term is inappropriate. The US was attacked on 7 Dec 1941 with no indications and warnings. The more appropriate term *when* the US is attacked will be *Electronic Blitzrieg*, combined arms warfare hitting hard and fast. The Government must either re-engineer an effective countermeasure, or develop a new one. Chapters 3 and 4, respectively, consider both.

Notes

[31] Note: Graph in Figure in upper left taken from Joint Publication 3-13: Joint Doctrine for Information Operations. Washington, DC., 9 Oct 1998, I-12.

[32] Sun Tzu. *The Art of War*. Edited and translated by Samuel B. Griffith. New York: Oxford University Press: 1971, 41.

[33] Executing couriers (from which we get the adage "Don't kill the messenger") was in fact an early form of information warfare, as was killing forward cavalry scouts before they could return to their encampment. As Total War emerged in part due to the resources provided by the *Industrial* Age, communication became critical. Thus, it became a capitol offense to kill and/or detain a courier carrying official dispatches. This reference is no analogy--the notion lives on in international laws that forbid tampering with either national technical means to verify treaty compliance or jamming communication lines between nuclear states.

[34] In January 2002, upwards of 27 several highly sophisticated listening devices (some even requiring SATCOM activation), were found aboard China's presidential aircraft, a new Boeing 767-300ER which Boeing was retrofitting under contract to Beijing. The Chinese have accused the US Government of planting the devices. Akin to when the US discovered the Soviets had planted hundreds of listening devices in the US Embassy in Moscow, the event caused little concern. A Chinese security expert noted: "This kind of thing is to be expected . . .Even if our relations were excellent, we would still spy on each other." (See: John Pomfret. "China Finds Bugs on Jet Refitted in U.S." *Washington Post Online*, 19 January, 2002, n.p. On-line. Internet, 3 February 2002. Available from http://www.taiwansecurity.org/WP/2002/WP-011902.htm.)

[35] Machiavelli agreed, noting "Nothing is more worthy of the attention of a good general than the endeavor to **penetrate the designs of the enemy**." [emphasis added.] (See: US Department of Defense. Joint Publication 3-13: Joint Doctrine for Information Operations. Washington, DC., 9 Oct 1998, I-19. Quote originally attributed to *Discourses*.)

[36] Sun Tzu, *The Art of War*.

[37] Hart went on to note "The predominance of the psychological over the physical, and its greater constancy, point to the conclusion that the foundation of any theory of war should be as broad as possible. . . . In most campaigns, the **dislocation of the enemy's psychological** and physical balance has been the **vital** prelude to a successful attempt at his overthrow."[37] (See: B.H. Liddell Hart.. *Strategy.* New York, New York: Penguin Group, 1991, 6.)

[38] Carl von Clausewitz. *On War*. Edited and translated by Michael Howard and Peter Paret. (Princeton NJ: Princeton University Press, 1976), 117.

[39] Antoine Jomini as well demanded organized espionage directing that a "general should neglect no means of gaining and multiplying sources of information, or overrelying on information based on demands for rigid perfection." Jomini likewise championed the pursuit of information while also recognizing its essential essence of accuracy. "One of the surest ways of forming good combinations in war would be to order movements only after obtaining perfect information of the enemy's proceedings. In fact, how can any man say what he should do himself; if he is ignorant what his adversary is about?"[39] He went on to delineate the "Principal Sources of Intelligence, including: "A

highly **organized e**fficient system of espionage, reconnaissance by **special** units, . . . systematic analysis of courses of action open to the enemy based on information, logic, and experience [and] Signals." (See: Antoine Henri De Jomini. *The Art of War.* London: Greenhill Press, 1996.)

[40] Department of the Air Force. *Air Force Doctrine Document 1. Air Force Basic Doctrine,* September 1997, 31-2.

[41] US Department of Defense. *Quadrennial Defense Review Report.* Washington DC: U.S. Government Printing Office, Sep 2001, 12.

[42] "China's IO/IW research is in the early stages of research. It currently focuses on understanding IW as a military threat, developing effective countermeasures, and studying offensive employment of IW against foreign economic, logistics, and C4I systems. Driven by the perception that China's information systems are vulnerable, the highest priority has been assigned to defensive IW programs and indigenous information technology development." (See: US Department of Defense. *Report to Congress Pursuant to the FY2000 National Defense Authorization Act: U.S. Report on China's Military Power (2000).* Washington D.C.: U.S. Government Printing Office, 2000, 3.)

[43] "Moreover, as the United States and other advanced nations more dependent on information technology in their military systems, they will become more susceptible to information warfare in operations. The revolution in military affairs places a bull's eye on the C4ISR that is critical to it. In the extreme, the ability of United States to project power and to strike at will could be undermined if an otherwise weaker enemy interfered with the links that network U.S. forces, fuse U.S. sensor data, and permit joint warfare." (See: Khalilzad, Aalmay M. and John P. White. *Strategic Appraisal: The Changing Role of Information in Warfare.* RAND: Project Air Force. Santa Monica, CA: 1999. 62-3.)

[44] "Information-intensified combat methods are like a Chinese boxer who has knowledge of vital body parts and can bring an opponent to his knees with a minimum of movement." (See: Clarence A. Robinson, Jr. : "China's Military Potency Relies On Arms Information Content." *SIGNAL Magazine*, November1999, n.p. On-line. Internet, 20 Dec 2001. Available from http://www.us.net/signal/Archive/Nov99/china-nov.html.)

[45] The Air Force is the only the service at this time exploiting the *asymmetric* nature of IO. Used asymmetrically, IO can be used to disable/harass conventional land, sea, air and space forces. The USA and the USN doctrine, however, are still centered around using IO symmetrically, that is, using IO is a weapon used only to negate adversary IO advantages.

[46] "Nations lacking military muscle could create an 'electronic Pearl Harbor' that could defeat the U.S. by using electronic warfare to cripple America's high-tech-dependent armed forces. [In addition] "For countries that could never win a war with the United States by using the method of tanks and planes, attacking the U.S. space system may be an irresistible and most tempting choice. ...," as noted in an official Chinese report entitled "The U.S. Military's Soft Ribs and Strategic Weaknesses," revealed by the official Chinese Xinhua news agency. Its content was authenticated by the American Foreign Policy Council (AFPC). (See: "China Threatens 'Electronic Pearl Harbor' Attack on U.S." *Infowar.com*, 11 October 2000, n.p. On-line. Internet, 6 January 2002. Available from http://www.Infowar.com/mil_c4i/00/mil_c4i_101100b_j.shtml).

Notes

[47] The Chinese consider information warfare to have both a *narrow* and a *broad* meaning, characterizing the US definition as "narrowly-focused," in that it is tied to "battlefield information warfare," the crux of which is "command and control warfare." Information warfare in the *broad* sense refers to warfare dominated by information in which digitized units use information [smart] equipment. The Chinese have a very ecumenical perspective on information warfare as well: noting "warfare has always been tied to information, it is only when warfare is dominated by information that it becomes authentic information warfare."[47] (See: US Department of Defense. *Report to Congress Pursuant to the FY2000 National Defense Authorization Act: U.S. Report on China's Military Power (2000)*. Washington D.C.: U.S. Government Printing Office, 2000, 4.)

[48] US Department of Defense. *Report to Congress Pursuant to the FY2000 National Defense Authorization Act: U.S. Report on China's Military Power (2000)*. Washington D.C.: U.S. Government Printing Office, 2000, 19.

[49] *U.S. Report on China's Military Power,* 15.

[50] Ibid, 19.

[51] "The Chinese infrastructure is significantly behind Western progress. The Chinese will therefore attack through the indirect approach, using asymmetric means as they can hope to win in a technology force-on-force match." (See: *U.S. Report on China's Military Power*, 10).

[52] *U.S. Report on China's Military Power*, 15.

[53] Ibid, 18.

[54] Ibid, 13.

[55] Ibid, 12.

[56] Ibid,17.

[57] Change Mengxiong. "The Revolution in Military Affairs: Weapons of the 21st Century." In *Chinese Views of Future Warfare.* Institute of National Strategic Studies. National Defense University. United States Government Printing Office: Sep 98, 11.

[58] Mengxiong, *Chinese Views of Future Warfare*, 54.

[59] *U.S. Report on China's Military Power*, 12.

[60] "China has the capability to penetrate poorly protected US computer systems and could potentially use CNA to attack specific US civilian and military infrastructures. This anti-access strategy is centered on targeting operational centers of gravity, including C4I centers, airbases, and aircraft carrier battle groups located around the periphery of China." (See: *U.S. Report on China's Military Power*, 14)

[61] Mengxiong, *Chinese Views of Future Warfare*, 54.

[62] Ibid, 20.

[63] Three of the anti-virus companies, which together represent 75% of the market for anti-virus software, had to provide virus samples to China's Ministry of Public Safety purportedly to test the software's capability. Finland refused to provide the samples and in fact, no other country has a similar requirement. The concern is not so much that Chinese would have viruses (many of which have antidotes), but that that by reverse engineering the viruses they will be able to jumpstart their CNA and CND programs. (See: Brudis, Ted. "China Extracts Computer-Virus Samples." *Wall Street Journal*, 30 March 2001, 12.)

Notes

[64] Mengxiong, *Chinese Views of Future Warfare* 54

[65] *U.S. Report on China's Military Power*, 9.

[66] "China Threatens 'Electronic Pearl Harbor' Attack on U.S." *Infowar.com*, 11 October 2000, n.p. On-line. Internet, 6 January 2002. Available from http://www.*Infowar.com*/mil_c4i/00/mil_c4i_101100b_j.shtml

[67] Ibid.

[68] Note similarity to Arab-Israeli Six-Day War where an outnumbered and outgunned Israeli combined-arms force dispatched a formidable Arab coalition in only six days by exploiting timing and tempo.

[69] *U.S. Report on China's Military Power*, 9.

[70] "China Threatens 'Electronic Pearl Harbor' Attack on U.S."

[71] Mengxiong, *Chinese Views of Future Warfare*, 11.

[72] *U.S. Report on China's Military Power*, 11.)

[73] Twenty-four USN seamen aboard an EP-3E ARIES II (Airborne Reconnaissance Integrated Electronic System II) spycraft were held for 12 days in Apr 2001 after being forced into an emergency landing after a mid-air collision severely damaged the 4-engine propeller-driven airplane. Chinese pilot Wang Wei had maneuvered his F-8 jet fighter aggressively into the path of the EP-3E, lost control, and struck the EP-3E aircraft over international waters. Wei perished when he could not recover his aircraft. The EP-3E, based on the venerable P-3 Orion frame is a SIGINT collector. The 12-day stand-off was predicated on an effective Chinese PSYOPS campaign which demanded an international apology from the US. The Chinese then broadcast an altered message once the US conceded.

[74] Timothy Shimeall et al. "Countering Cyberwar." *NATO Review*, Winter 2001/2002, 1.

[75] General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. Report GAO/T-AIMD-96-92, 22 May 96, 30.

[76] FBI and CERT both believe the number of attacks that go *un*reported is close to 80-93%. Most attacks go unreported because of the negative publicity involved.

[77] This is in fact the art of maneuver warfare--leaving an adversary no options but the one desired where the aggressor can use its strengths against him.

[78] GAO, *Computer Attacks at Department of Defense Pose Increasing Risks,* 7.

[79] In the videotapes sent subsequent to 9/11, Osama Bin Laden stated that the US economy was his real target, noting: "…if the US economy suffers enough, Americans will withdraw from [the Mideast.]" (See: "Bin Laden says US Economy Was Target." *CNN.com*, 28 December 2001, n.p. On-line. Internet, 3 February 2002. Available from http://www.cnn.com/2001/WORLD/asiapcf/central/12/27/ret.bin.laden.tape/.)

[80] *Intrusion Detection and Prevention Product Update*. Presentation, Cisco Industries. San Jose: CA, 12 Dec 2000. On-line. Internet, 4 February 2002. Available from http://www.cisco.com/networkers/nw00/pres/2505.pdf.

[81] This continuum is particularly perplexing in that different bodies of law come into affect given the intention and actors. Col Dunlap writes: ". . . a covert peacetime Information Operation directed against non-state actors (e.g., terrorists or drug dealers) is subject to a rather different body of law than psychological operations (psyops)' aimed

against lawful combatants in an international armed conflict. The aforementioned phrase "international armed conflict" is itself of great import. As a general rule, LOAC-like most international law-applies to relations between nations, not individuals or other non-state actors." (See: Vasquez, John A. "Conceptualizing War." In *Nature of War Coursebook Academic Year 2002*. Compiled by Col(s) Jim Forsyth PhD, et al. Air Command and Staff College: Department of International Security and Military Studies. Maxwell, AFB, AL. Aug 2001, 5. and Campen, Alan D., and Douglas H. Dearth. Cyberwar 3.0: Human Factors in Information Operations and Future Conflict. AFCEA International Press. Fairfax VA, Oct 200, 139.)

[82] Security experts refer to viruses and worms using standard military terms as well. The email containing the virus/worm is the **vector**, the virus/worm is the **payload**, and it attacks a given **target**.

[83] Most subject lines containing Cyber warfare payloads have fairly obvious subject lines, e.g. "I Love You," "Naked Pictures of xxx, etc. Nimda's subject line, however, sounded legitimate, urgent, and friendly: "Antivirus companies warn that an e-mail message asking for peace between America and Islam actually carries an extremely malicious and destructive payload." (See: "Worms continue Internet attacks," MSN.com, 25 September 2001, n.p. On-line. Internet, 20 December 2001. Available from http://news.com.com/2009-1001-273186.html?legacy=cnet.)

[84] Elinor Abreu. "Damage from Code Red worms continuing to add up." *Infoworld.com*, 8 Aug 2001, n.p. On-line. Internet, 20 December 2001. Available from http://iwsun4.infoworld.com/articles/hn/xml/01/08/08/010808hnredcosts.xml.

[85] "'Code Red' impact felt at major companies." *CNN.com*, 9 August 2001, n.p. On-line. Internet, 20 December 2001. Available from http://www.cnn.com/2001/TECH/internet/08/09/code.red/.

[86] Paul Festa and Joe Wilcox. "Experts estimate damages in the billions for bug." CNET.com, 5 May 2000, n.p. On-line. Internet, 20 December 2001. Available from http://news.cnet.com/news/0-1003-200-1814907.html.

[87] Anthony Kimery. "Moonlight Maze." *MIT-KMI.com,* 3 Dec 99, n.p. On-line. Internet, 20 December 2001. Available fromhttp://www.mit-kmi.com/3_6_art1.htm.

[88] The four IOPs are Centers of Gravity, and within them have several nodes, some of which were delineated in PDD 63 (e.g. electrical grid, telecommunications, etc.) Although the US will never know for sure the full extent of the 9/11 attacks planned by Bin Laden, it is obvious that they were centered on symbols of the IOPS--the World Trade Center (Economic), the Pentagon (Military), and potentially the White House or Capitol (Diplomatic). No known attack on the Information IOP has been detected. Each of the IOPs are mutually supporting, but the heavier arrows (at termination) highlight which IOP is more dependent on its corresponding IOP. For example, the military IOP is more dependent on the diplomatic element in that the military has civilian masters, yet the military provides the diplomatic IOP the deterrent/direct force to enact is policies. The borders on each of the IOPs likewise show the degree of vulnerability. Therefore, it indicates the most likely attack method to be employed. The Military IOP, given the US's overwhelming dominance and being the only remaining superpower, can be considered nearly impenetrable at this time. Likewise, both the Economic and Diplomatic IOPs re-

main fast--the US dollar remains the world currency standard, and again, the US is the only superpower. The spring represents the dynamic natures of both the international environment and democracy in action--each of the lines are flexible and like a spring when compressed or extended from its neutral position, provides a restoring force to remain in equilibrium, pushing and pulling on each of the other IOPs as necessary to maintain the balance of power. This restoring force is likewise governed by a damper (as observed by Major Greg Reiter) which controls the speed of the restoration much like a shock absorber does in a car. Its parameters are governed by other factors. For example, the US's approach toward Israel in the current Mideast conflict could have been more rapid but the administration chose to move cautiously. The cloud represent the dynamic, unpredictable nature of the international environment which changes the IOP calculus.

[89] The FBI recently uncovered a virus that "revealed a computer virus that can erase hard drives and dial 911 emergency systems." The virus causes "victim systems to dial 911, possibly causing emergency authorities to check out substantial numbers of 'false positive' calls." 89 The initial attack was centered in Houston, and while quickly contained, did manage to affect four of the nation's largest Internet providers: America Online, MCI WorldCom, AT&T and NetZero. The 911 aspect is particularly disconcerting with respect to a terrorist attack, and the ensuing fog and friction both at the military and civil authority level, especially considering the National Guard and Reserve forces serve both. (See: "New virus can wipe out hard drives." *CNET.com*, 2 Apr 2000, n.p. On-line. Internet, 26 December 2001. Available from http://news.cnet.com/news/0-1005-200-1623077.html?tag=rltdnws.)

[90] The White House. *A National Security Strategy for a Global Age*. Washington DC: Office of the White House, December 2000, 24.

[91] The four IOPs are Centers of Gravity, and within them have several nodes, some of which were delineated in PDD 63 (e.g. electrical grid, telecommunications, etc.) Although the US will never know for sure the full extent of the 9/11 attacks planned by Bin Laden, it is obvious that they were centered on symbols of the IOPS--the World Trade Center (Economic), the Pentagon (Military), and potentially the White House or Capitol (Diplomatic). No known attack on the Information IOP has been detected.

[92] Computer security experts at CERT agree, noting: "Information and communication technologies have been embraced enthusiastically but with little attention to attendant, if inadvertent, vulnerabilities. **Indeed, reliance on the new systems has grown much faster than our grasp of the vulnerabilities inherent** in the networks, systems and core technologies that underlie the information and communications revolutions." (See: Phil Williams, et al. "Intelligence Analysis for Internet Security." Carnegie-Mellon Software Engineering Institute. Available on-line. Internet at http://news.cnet.com/news/0-1003-200-1814907.html).

[93] Note: The original chart from 95-053 was used as a baseline, and modified for the Information IOP and the changing calculus of the international environment. (See: "ACSC Research Project 95-053: Planning and Execution of Conflict Termination." In Air Command and Staff College Distance Learning Program. Lesson Wc503r05. CD-ROM ACSC Multimedia Edited Version 2.2., Aug 1997, n.p.)

Notes

[94] "Heading Off an 'Electronic Pearl Harbor': CEOs, policy leaders discuss cyber-security at forum." *CNN.com*, 6 April 1998, n.p. On-line. Internet, 24 December 2001. Available from http://www.cnn.com/TECH/computing/9804/06/computer.security/.

[95] Michael J. Miller. "The Cyberterrorism Threat." *pcmag.com*, 27 Nov 2001, n.p. On-line. Internet, 21 December 2001. Available at http://www.pcmag.com/article/0,2997,s%253D1499%2526a%253D17512,00.asp.

[96] Terril D. Maynard, a CIA analyst attached to the NIPC emphasized that: "The use of untested foreign sources for Y2K remediation has created a unique opportunity for foreign countries or companies to access and disrupt sensitive national security and proprietary information systems." (See: Anthony Kimery. "Moonlight Maze." *MIT-KMI.com,* 3 Dec 99, n.p. On-line. Internet, 20 December 2001. Available from http://www.mit-kmi.com/3_6_art1.htm.) Note: This is not the "super-secret" espionage it appears to be. In 1997, Intel® was widely criticized when it was revealed it had written code into its processors that could identify the user and their search patterns for subsequent consumer targeting. Another example is the infamous Clipper Chip, a communication chip whose encryption system was to be managed by the NSA and forcefully rejected. In addition, PDD 63, "The Clinton Administration's Policy on Critical Infrastructure Protection" concluded that although the danger was not imminent, the US "infrastructures [were] **increasingly dependent** on information and communications systems that criss-cross the nation and span the globe. That dependence is the source of **rising vulnerabilities** . . . We did find widespread capability to exploit infrastructure vulnerabilities. **The capability to do harm—particularly through information networks--is real; it is growing at an alarming rate; and we have little defense against it** [emphasis added.] (See: President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* Office of the President. Washington DC: US Government Printing Office, October 1997, i.)

[97] John Arquilla and David Ronfeldt. *In Athena's Camp*. (Santa Monica: RAND National Defense Research Institute, 1997, 178.

[98] The Air Force is considering increasing the power on the GPS IIF satellites due to this vulnerability (See Appendix B), even to the extent that it will delay the acquisition of GPS III.

[99] Del Vecchio noted: "Both government and industry **have viable concerns whether or not their messages are both secure from an adversary** as well as to the reliability of the message reaching its destination. …**Today's PSTN's may have security and reliability risk due to the path a message may be sent** . . .[s]ince many government agencies use Public Switched Telephone Networks (PSTN) for official voice messages. . . "[emphasis added.] Currently, the Department of Defense (DoD) relies on the Public Switched Telephone Networks (PSTN) for the bulk of its telecommunications. The PSTN is a composite of multiple interconnected networks, where each network is operated, maintained, and managed independently from the others. …However, the network operators … rely a great deal on each other for routing calls to destinations outside of their network span. Based on worked out agreements among the service providers, they decide on how and where they will physically interconnect their networks. These physical points of interconnection are called Points of Presence (POPs). In today's world

Notes

of the telecommunications, there is much concern with the reliability and security of a given network. (See: Capt Jeffrey R. Del Vecchio, "An Incentive Model for Secure International Telecommunications." Thesis. Presented to Department of Systems and Engineering Management Graduate School of Engineering and Management Air Force Institute of Technology. Air University. Air Education and Training Command. March 2000, 22)

[100] The more significant concern is that the DoD is unaware of the vulnerability of its systems--again thinking in Euclidean terms. The caller imagines the line being connected directly from his office to the other party's handset, unaware of the fact that call can be carried over multiple lines, multiplexed, sent over SatCom, fiber, copper, or submarine cable, and may even pass through foreign gateways.[100]

[101] Unlike space, offensive information weapons have been used. Space has no force projection capability, save for the ground-ground attack method employing ICBMs.

[102] Classic Psyops and the media precluded use as junta resistance collapsed.

[103] As noted by LtGen S. Bogdanov, Chief of the General Staff Center for Operational and Strategic Studies (FSU): "Iraq lost the war before it even began. This was a war of intelligence, EW, command and control, and counterintelligence. Iraqi troops were blinded and deafened. Modern war can be won by informatika and that is now vital for both the US and USSR." (See: US Department of Defense. Joint Publication 3-13: Joint Doctrine for Information Operations. Washington, DC., 9 Oct 1998, II-15.

[104] Thomas Keaney and Eliot A. Cohen. *Gulf War Air Power Survey Summary Report*. (Department of Defense. Washington D.C., 1993), 248.

[105] They include Senators Sam Nunn and Dianne Feinstein, Marv Langston (former deputy CIO for the Department of Defense (DoD), and former Deputy Secretary of Defense John Hamre.

Chapter 3

Mission Threat Analysis: The Need

Critical operational goals provide the focus for DoD's transformation efforts: Assuring information systems in the face of attack and conducting effective information operations, denying enemies sanctuary by providing persistent surveillance, tracking, and rapid engagement, enhancing the capability and survivability of space systems, and leveraging information technology and innovative concepts to develop an interoperable, joint C4ISR architecture.

—2001 Quadrennial Defense Review

Those at the tip of the spear do not care where their information comes from . . .[t]o the special operator who is trying to help guide a bomb to a target, it is of no consequence that the target's coordinates came from a satellite, E-8 Joint STARS aircraft, or Predator unmanned aerial vehicle. He simply wants the target destroyed-and fast.

—Gen John P. Jumper, Chief of Staff, USAF

Chapter 2 established the scope of the threat as broad, enduring and growing. In keeping with the Mission Needs Statement construct, the second element of a MNS also describes the mission need/deficiency in terms of its objectives, capabilities and doctrine. This chapter identifies the deficiency as a dogmatic perspective that has thus far failed to recognize the inherent synergies between symbiotic elements of IO resulting in conflicts between service and joint doctrine. It further asserts this conflict will continue to affect proper development, maturation, and execution of the countermeasure necessary to defeat the IO threat.[106] This chapter then posits a unifying definition for IO based on the QDR's visionary and directive guidance to eliminate the deficiency.

Objective. Fig. 8 represents the fact that definitions begin with objectives which evolve into doctrine. Definitions are critical. Vasquez noted that

> "In defining a word, one may be doing a lot more than one suspects." Further, he noted that [because] "everyday definitions are derived from cultural experience rather than scientific analysis, it is highly unlikely that they will live up to this task."[107]

In fact, "everyday" definitions and Service-specific "culture" are the *very* reasons disparate terms have emerged and an effective IO strategy remains undeveloped. Yet the DoD has failed to name an executive agent to manage this growing area, repeating the same strategy it employed for the space mission area for almost two decades. That hesitance resulted in confusion, costly inter- and intra-service/agency rivalries, overlap, and operational shortfalls, and a fractured space community.[108] The DoD cannot afford a similar policy toward Information--it has skipped Steps 2 and 3 (Figure 2), and moved directly to execution. As a result, IO strategies have failed in their ultimate promise in the conflicts articulated above. A lead service must define new constructs scientifically vice culturally to enable its doctrine to properly steer force planning, equipping, organizing, and training forces, and consider the implications to the Law of Armed Conflict (LOAC), an acutely pertinent concern with the April 2002 ratification of the International Criminal Court[109] and the US's growing international dominance and consequent role.

Without a solid definitional construct, the DoD has been--and will continue to be--unable to focus its forces and achieve unity of action[110]--a concept relevant to *any* activity, not just battle. For example, the USAF has adopted the term *CounterInformation* as an analog to its air and space superiority roles (*CounterAir* and *CounterSpace,*[111]) replacing established joint definitions with its air-centric doctrine. General Bob Gaskin, the Air

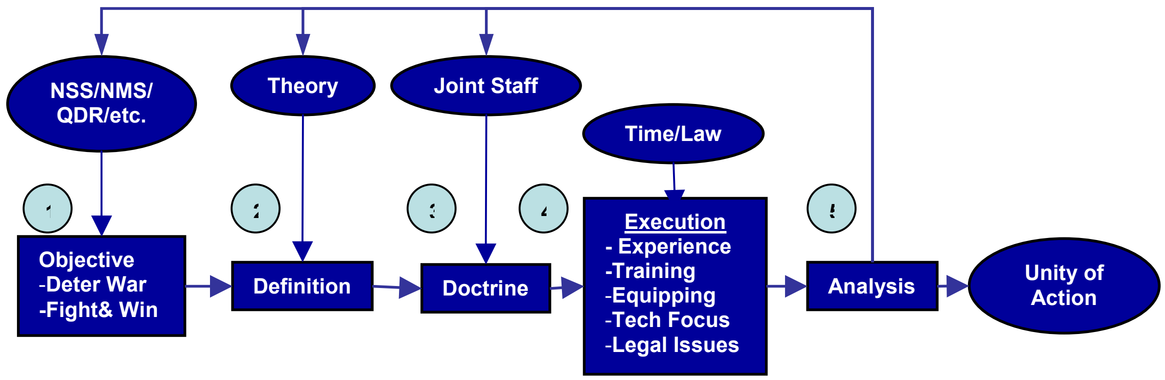


Figure 8: Unity of Action Begins with Known Objectives and Solid Definitions

Force 4-Star in charge of doctrine in the late 1990s, commented as well that:

> "Everybody trains, organizes, equips, to their service doctrine . . . [w]hen the service comes to war, they come with their service doctrine, not a joint doctrine."[112]

The Army does not even accept that the DoD has entered into an "Information Age," and both it and the Navy construct IO around symmetric attacks (i.e. IO against IO) and myopically focus on cyberwarfare. JP 3-13's construct for IO is also problematic, in that it only states that IO "may include . . . CNA"[113] and does not even consider CND a part of Defensive IO.[114] The QDR is clear in this regard:

> "The [DoD] must also align, consolidate, or differentiate ***overlapping*** functions of [OSD], the Services, and the Joint Staff. To do this, DoD will develop recommendations to eliminate redundancy[emphasis added.]"[115]

Definitions. Joint definitions should be rooted in the central purpose of the military--to fight the nation's wars, as well as *the way* wars are fought and for *what purpose*. Clausewitz wrote "War is politiks by other means"[116] where the literal translation of *politik* is a triumvirate of "politics, policy, and history of the nation."[117] Therefore each instrument of war must comply with those three aspects to ensure the integrity of the political **Objective**. The President states his international perspective (the *political* element) in the NSS, which explains the criticality and vulnerability of the IT infrastructure.[118] *Policy* is instantiated in various policy documents, including the NSS, NMS and QDR. The QDR delineates six goals, summarized in Table 4, all of which are dependent

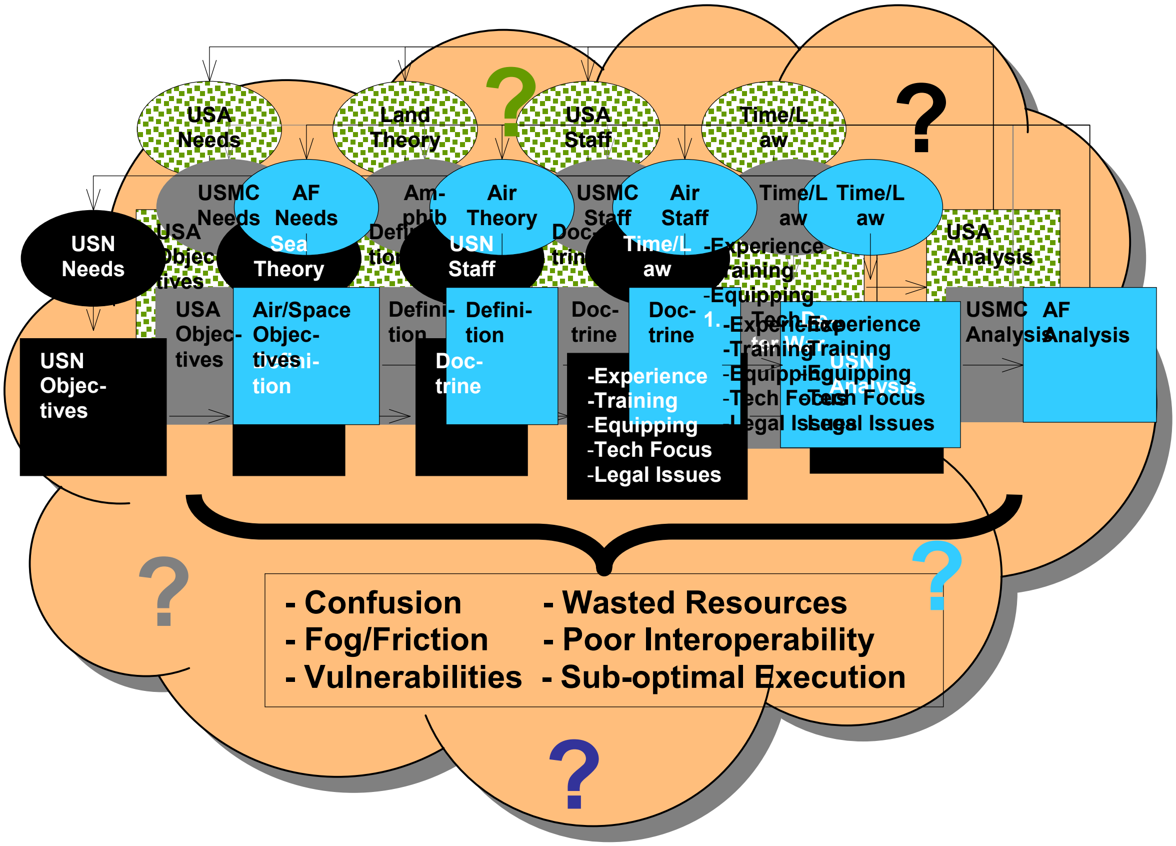


Figure 9: Overlapping/Conflicted Concepts Fail to Achieve Unity of Action

on information, and four of which (2, 4, 5, 6) have information as their **central, pervasive** tenet. Finally, **history** is replete with examples of the criticality of information as shown in Chapter 2 and in the QDR.[119.] Having met the three tenets of *politik*, the definitional requirements to truly execute the IO weapon of war as a political instrument, can be derived.

Table 4: Definitional Construct Based on IO Objectives Dictated by US Politik

Source	IO Objective	Connection to Information
NSS	**Politics:** "Critical infrastructures, including telecommunications, energy, finance, transportation, water, and emergency services, form a bedrock upon which the success of all our endeavors -- economic, social, and military--depend. We must understand the vulnerabilities and interdependencies of our infrastructures. . ." [120]	**Therefore, the definition of IO must:** **- Recognize Information's contribution to all IOPs** **- Recognize totality of Infosphere**
QDR Goal # 1	**Policy:** "Protect bases of operation at home and abroad and defeat the threat of CBRNE weapons."[121]	- DoD to support state/local officials - Exquisite intelligence - Rapid, reliable C4ISR between ISR and TBM assets
QDR Goal #2	**Policy: "Assure information systems in the face of attack and conduct effective information operations"**[122]	- IO provide the means to rapidly collect, process, disseminate, and protect information while denying these capabilities to adversaries. - Influence perceptions - Perform CNA/CND - Conduct EW - Defines IO as core competency - Demands DoD develop an integrated approach **Therefore, the definition must:** **- Provide for a Defensive component** **- Provide for an Offensive component**
QDR Goal #3	**Policy: "Project and sustain U.S. forces in distant anti-access and area denial environments"**[123]	- Deception - Rapid Logistics - Exquisite Intelligence - Defeat long-range means of detection
QDR Goal #4	**Policy: "Deny enemies sanctuary by providing persistent surveillance, tracking, and rapid engagement."**[124]	- Capability to find and strike protected enemy forces - Limit collateral damage - Bolster ISR investments - Emphasis on UAVs - SOF need for enhanced ISR - Additional emphasis on comm **Therefore, the definition of IO must:** **- Provide for Symmetric Warfare** **- Provide for Asymmetric Warfare** **- Provide for a Support Role**
QDR Goal #5	**Policy: "Enhance the capability and survivability of space systems."**[125]	- Space is a vital interest and therefore a friendly COG - Space assets offer an asymmetrical target which can disrupt US "economic and societal stability, and national will" - Space surveillance is foundation - Must enhance C2 - Pursue Space control **Therefore, the definition of IO must:** **- Recognize Information's contribution to all IOPs**

Table 4 (Cont.): Definitional Construct Based on IO Objectives

Source	IO Objective	Connection to Information
QDR Goal #6	**Policy: "Leverage information technology and innovative concepts to develop interoperable Joint C4ISR"**[126]	- IT is key foundation to transformation - Demand for interoperable comm - Interoperability is key element - Backward compatibility for legacy systems - Focus on end-to-end C4ISR - Exploit out current advantages **Therefore, the definition of IO must:** **- Provide for Analog Data exchange** **- Provide for Digital Data Exchange** **- Include C4ISR/requisite interoperability** **- Have information as a central tenet**
QDR	**Policy:** "A multifaceted approach to deterrence is needed. [It] requires forces and capabilities that provide the President with a wider range of military options to discourage aggression or any form of coercion."[127]	**Therefore, the definition of IO must:** **- Recognize totality of Infosphere** **- Be applicable across the conflict spectrum from peace, through MOOTW, to MTW** **- Contain graduated levels of exploitation**
QDR	**Policy:** "A central objective of the review was to shift the basis of defense planning from a "threat-based" model that has dominated thinking in the past to a "capabilities-based" model for the future."[128]	**Therefore, the definition of IO must:** **- Be effects based**
QDR	**Policy:** "This transformation will be conducted in a timely but prudent manner. …prudence dictates that those legacy forces critical to DoD's ability to defeat current threats must be sustained as transformation occurs. Consequently, while emphasizing transformation, DoD will also selectively recapitalize legacy forces."	- Radical transformation is critical. The DoD needs to continue to accelerate it to optimize its promise - The DoD cannot move so fast toward the future that it abandons current capability - Recognize the need for new organization, force structures, and systems **Therefore, the definition of IO must:** **- Improve/not abandon current concepts** **Therefore, the definition of IO should:** **- Embrace new organizational constructs**
QDR	**History:** "Kosovo underscored the need for high-capacity, interoperable communications systems that can rapidly transmit information over secure, jam-resistant datalinks to support joint forces."[129]	- High capacity - Multiple transmission mediums - Interoperability **Therefore, the definition of IO must:** **- Provide for Analog & Digital exchange** **- Include C4ISR/requisite interoperability**
Ch 2	**History:** Multiple threats across the spectrum of actors, time, conflict, and IOPS.	**Therefore, the definition of IO must:** **- Be applicable across all threat domains** **- Be long-term** **- Contain graduated levels of exploitation**
Future	- USAF taking on increased role	- Future threat vs. capability violates span of control See Chapter 4 for details **Therefore, the definition of IO must:** **- Have nominal span of control**
Joint Doctrine	**Policy:** Space provides information	**- Therefore, the definition of IO must:** **- Recognize true contribution of space**

Definition. Table 4 delineates the required/desired attributes of the definition of IO. Being multi-faceted, an umbrella concept is necessary. Concepts abound: Command and Control Warfare (C2W), IO, Information Superiority, Information Warfare (IW), C4ISR, and Electronic Warfare (EW). As shown in Table 5, however, each of these are deficient in that they fail to incorporate the comprehensive thrust of the QDR without eliminating redundancies or filling current gaps. Figure10 portrays this "kill-chain" hierarchy, demonstrating **information** becomes both an enemy and a friendly CoG and therefore has both an offensive and defensive component--e.g. CND is the *protection* analog of the CNA *offensive* mechanism.[130] Furthermore, this hierarchy and its elements (the spikes) pervade Warden's five rings, bridging his ring and other nodal models. Simply stated, IO

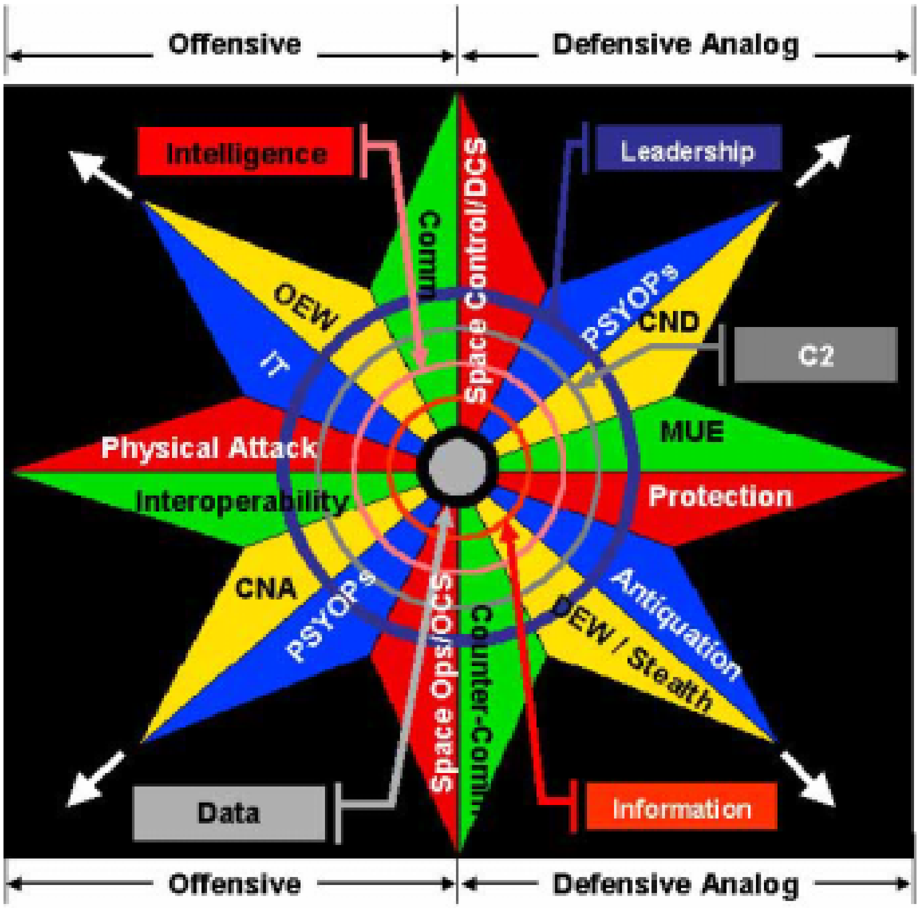
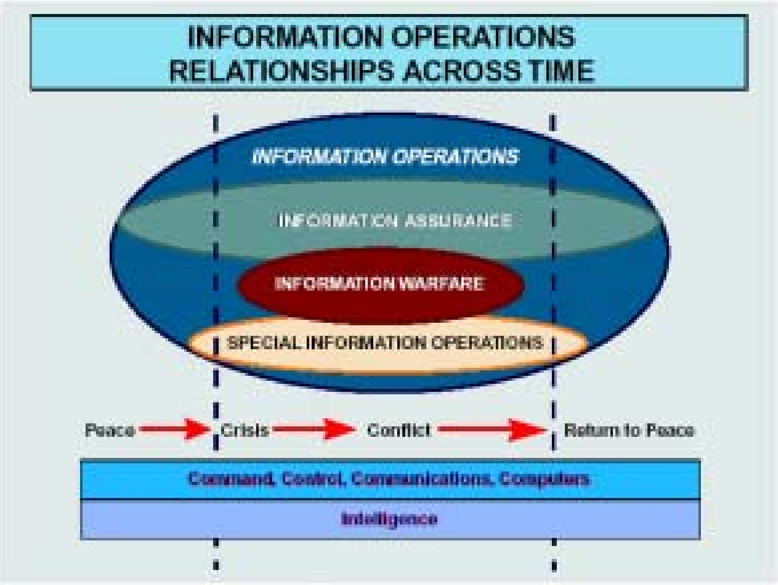


Figure 10: Expansion of Warden's Inner Ring with respect to Information Ops

provides and protects many and myriad sources of **data**, which when processed by machine or human becomes **information**, which upon analysis becomes **intelligence**. This throughput is aided by **information technology** (IT, including computer hardware, software, etc.) and other peripherals necessary for **communication** which commanders use to organize and **command and control** their forces. Communications all employ the electromagnetic spectrum (EM) and/or electric/electronic connectivity. **Thus, it's not the *hardware* or *source* that's important--it's the *information they carry*, that is the actual objective, effect-based target.**


INFORMATION OPERATIONS RELATIONSHIPS ACROSS TIME
INFORMATION OPERATIONS
INFORMATION ASSURANCE
INFORMATION WARFARE
SPECIAL INFORMATION OPERATIONS
Peace
Crisis
Conflict
Return to Peace
Command, Control, Communications, Computers
Intelligence

..

Figure 11:The Definition of IO is Constrained to Crisis/Conflict[131]

Comparing these umbrella concepts discussed above in tabular form (Table 5) for ease, deficiencies are striking. For example, the current joint definition of IO--"Actions taken to affect adversary information and information systems while defending one's own information and information systems--conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries,"[132] is incomplete in that by definition it is applicable only during crisis/conflict[133] (Fig. 11). JP

3-13's construct for IO is also problematic, in that it only states that IO "may include . . . CNA."[134] And JP 3-13 does not even consider CND as a part of Defensive Information Operations. Finally, EW is insufficient in that it is constrained to the EM spectrum, and thus cannot fully encompass CNA/CND operations. Similarly, the terms cyberwarfare and net warfare are likewise incomplete as they are centered on computer systems and software. **Of most concern, however, is the stove-piped construct within which each of these fields lie.** Understanding what must be done to *attack* information, highlights what must be done to protect *information*. Unfortunately, the fields of C4ISR and IO have been segregated. Electronic warfare and information operations have also been segregated. This is particularly troublesome given that EW is governed by the same laws in all environments--sub-surface, air, and space.[135] This fact alone makes achievements in ground-based, aircraft-based, and eventually space-based jammers invaluable to all. Finally, USAF terms for information operations, information warfare, and information superiority differ from those of joint doctrine, which should take precedence. The result is wasted resources, lack of interoperability, and increased fog and friction.

Nor does the USAF follow its own joint doctrine consistently with respect to space, betrayed mainly by 1) the need for space to remain within the purview of the USAF and 2) a *medium* vice *effect* mentality, an artifact of the Constitutionally-derived, geographically-based separation of service roles. This Euclidean-based, land-sea-air-space handicap, likewise codified in the UCP and JP 3-33, was also criticized by Secretary Rumsfeld referring to it as "old think" and "too regionalized."[136] This regionalized mindset unfortunately obscures space operations fundamental **capability** and **effect**--space operations are fundamentally a subset of information operations

This premise is not only a product of physics and current use, but follows from joint and service doctrine which clearly and correctly characterize the contribution of space assets. For example, AFDD 2-2 **consistently** describes space systems as information sources: “Space systems provide . . .timely, accurate, and reliable **space-derived information, data products, and services**.”[137] And although USAF leadership has not stated that space is a subset of information, several comments intimate they too consider space to be composed of enabling information assets. Space assets are simply information sources, and will remain so for the definable future--their utility is derived from the **data** they downlink. Once satellites execute their payload, the satellite fundamentally becomes a communications satellite,[138] whether it’s a platform for all-spectrum imaging,[139] collecting signals, detecting launches, providing navigation, or relaying communications.

The QDR likewise emphasized offensive and defensive space control, noting such activities were necessary to protect the “US national **information** infrastructure.”[140] Space control methods will revolve around EW techniques. Consortium use, international repercussions, and the permanent effect of orbital debris in the most cherished orbital regimes will preclude the use of kinetic type weapons.[141] The AF’s embryonic space control efforts "focus only on negation technologies which have temporary, localized and reversible effects."[142] This is consistent with remarks from Gen Estes, who explained that space control was not about “destroying space assets of other nations, but negating them, stopping them for a period of time.”[143] As such, the resulting definition of Information Operations must be include the contributions of space. Future space control weapons only target *spaced-based/space-derived information sources*, whereas the data carried may traverse multiple ground lines, cable, fiber, telephony, and/or multiple satellite "hops." Cable and fiber lines are being installed at an exponentially growing rate--not so with the satellite industry now plagued with multiple bankruptcies, expensive and vulnerable service, and disenchanted investors. Finally, targeting a system just because it resides in space is *input-based*, not *effects-based* (and certainly not capability based, as demanded for all future procurements vis-a-vis the QDR) and leads to myopic targeting, obscures redundant paths and automatic fall-overs, and eventually leads to antiquated stove-piped, Euclidean-based acquisitions.

Synthesizing the key aspects of these definitions to meet the needs to promulgate the QDR direction, a new definition of Information Operations can be constructed:

> "Continuous military operations conducted within the Infosphere that enable, enhance, and protect US capabilities to collect, process, and act on information through a deliberate, integrated C4ISR architecture to achieve symmetric and/or asymmetric advantages across the full range of actions required by all national instruments of power in support of national security objectives."

Table 5: Definition Conflict

Element	Information Operations	Information Warfare	Information Superiority	Information Dominance
	Actions taken to **affect adversary** information and information systems while **defending** one's **own** information and information systems.	**Information operations** conducted during **time of crisis or conflict** to achieve or promote specific objectives over a specific **adversary** or adversaries.	That degree of **dominance** in **the information domain** which permits the conduct of operations without effective opposition	The **degree** of information **superiority** that allows the possessor **to use information systems** and capabilities to achieve an operational advantage in a conflict or to control the situation **in operations other than war** while denying those capabilities to the adversary
- Recognize Infosphere	NO	NO	YES	YES
- Information as central tenet	YES	YES	YES	YES
- Recognize all IOPs	NO	NO	NO	NO
- Symmetric war	YES	YES	YES	YES
- Asymmetric war	NO	NO	NO	NO
- Analog data	NO	NO	NO	NO
- Digital data	YES	YES	YES	YES
- Include C4ISR	YES	YES	YES	YES
- Defensive	YES	YES	YES	YES
- Offensive	NO	NO	NO	NO
- Support Role	NO	NO	NO	NO
- Nominal span of control	YES	YES	YES	YES
- Applicable in peace	NO	NO	YES	YES
- Applicable in war	YES	YES	YES	YES
- Applicable at any time	YES	NO	YES	YES
- Recognize space as simply information conduit	NO	NO	NO	NO
- Graduated levels of exploitation	YES	YES	NO	NO
Is effects based	NO	NO	NO	NO
Key Deficiencies	- Fails to recognize EW - Works only in Conflict	- Fails to recognize EW - Works only in Conflict - Works only during a specific crisis -It's an end state	- Fails to recognize EW - Works only in Conflict - Tautological -It's an end state	- Fails to recognize EW - Works only in Conflict - Tautological -It's an end state

Table 5: Definition Conflict (Cont.)

Element	EW	C2 Warfare	Computer network attack	Computer network defense
	Any military action involving the use of electromagnetic and directed energy to control the EM spectrum or to attack the enemy.	Integrated use of OPSEC, deception, PSYOP, EW, and physical destruction, supported by intel, to deny information to, influence, degrade, or destroy adversary C2	Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves	Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction
- Recognize Infosphere	**NO**	**NO**	**NO**	**NO**
- Information as central tenet	**NO**	**NO**	**YES**	**YES**
- Recognize all IOPs	**NO**	**NO**	**NO**	**NO**
- Symmetric war	**YES**	**YES**	**YES**	**YES**
- Asymmetric war	**NO**	**YES**	**NO**	**NO**
- Analog data	**YES**	**YES**	**NO**	**NO**
- Digital data	**NO**	**YES**	**YES**	**YES**
- Include C4ISR	**YES**	**NO**	**NO**	**NO**
- Defensive	**YES**	**YES**	**NO**	**YES**
- Offensive	**YES**	**YES**	**YES**	**NO**
- Support Role	**YES**	**YES**	**YES**	**YES**
- Nominal span of control	**YES**	**NO**	**YES**	**YES**
- Applicable in peace	**NO**	**NO**	**NO**	**YES**
- Applicable in war	**YES**	**YES**	**YES**	**YES**
- Applicable at any time	**NO**	**NO**	**NO**	**NO**
- Recognize space as simply information conduit	**POSSIBLE**	**NO**	**NO**	**NO**
- Graduated levels of exploitation	**YES**	**YES**	**YES**	**YES**
Is effects based	**NO**	**YES**	**YES**	**YES**
Key Deficiencies	- Fails to recognize totality of Infosphere - Fails to recognize digital data exchange	- Fails to recognize totality of Infosphere - Too Broad- Good “effects-based” concept, but indescript - Does not include totality of C4ISR	- Fails to recognize totality of Infosphere - Centered on computers only - Centered on offensive ops - Does not include totality of C4ISR	- Fails to recognize totality of Infosphere - Centered on computers only - Centered on defensive ops - Does not include totality of C4ISR

The term Infosphere then must be defined. Using a similar process as above, Table 6 provides the requisite definition, showing the shortfalls of the current concepts.

Table 6: Defining the Battlespace

Term	Origin	Definition	Shortfalls
Cyberspace$_1$	JP 1-02	"the **notional** environment in which digitized information is communicated over computer networks [emphasis added.].[144]	- Notional - Fails to account for analog environment - Focused on computer systems only
Cyberspace$_2$	LtCol Rattray	"man-made environment for the creation, transmittal, and use of information in a variety of formats . . .and consists of electronically powered hardware, networks, operating systems, and transmission standards"[145]	- Man-made fails to account for EM spectrum - Focused on computer systems only
Defense Information Infrastructure	JP 1-02	The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving Department of Defense (DOD) local, national, and worldwide information needs."[146]	- Focused on defense only, and the vast majority of networks under attack do not belong to the defensive establishment - A priori requirement for being interconnected when many DoD systems are in fact, not
Information Environment	JP 1-02	"The aggregate of individuals/organizations, or systems that collect, process, or disseminate information; [including] the information itself."[147]	- Includes personnel which--a concern for LOAC and Posse Comitatus if targeted
Infosphere	Derived	"the rapidly growing global network of military and commercial C4ISR and networks linking information data bases and fusion centers, including the EM spectrum, that are accessible to the warrior anywhere, anytime, in the performance of any mission; provides the worldwide automated information-of-exchange backbone support to joint forces; and provides seamless operations from anywhere to anywhere that is secure, flexible, adaptive, and transparent to the warrior."	- None

Summary. Locking down definitions is not a matter of semantics. Designating a lead service is not a matter of politics. Defining the operational environment is not a matter of rice bowls. Given the scope of the threat, this chapter posited a unifying concept and joint definitions for both "Information Operations" and the "Infosphere" based on the fundamental objective of war and centered on national security objectives, vice the conflicted definitions borne from disparate cultures. With common objectives and definitions, one ultimately can achieve Unity of Action. Unity of action is a key component of Unity of Effort. But Unity of Effort requires Unity of Command as well and thus far, civilian leadership has failed to define that lead. Chapter 4 will prove that a new service is needed to provide that Unity of Command, and thus finally achieve Unity of Effort.

Notes

[106] Several excellent papers/articles/etc. have been written regarding this definitional conflict. They have legitimately argued the point from a service vice joint doctrinal conflict. But the conflict remains unresolved. A failure to execute IO during Operations Restore Democracy, Deliberate Force, and Enduring Freedom have been attributed to a failure to coalesce a definition, while leaving the US open to the psychological aspect of IO in Somalia, Haiti, and Bosnia. Therefore the author took the approach to ascertain the fundamental reason why this conflict should be a concern, and why IO has failed to live to its promise, and why it will continue to fail.

[107] Heisenberg's principle states that it's impossible to determine simultaneously both the position and the velocity of a particle. In other words, once something is observed, its fundamental nature is changed simply because it was observed. So too was the concern when the DoD coined the term formation Warfare in early 1990, irritating the international community (particularly the Chinese), in that the term connoted that the United States, a nation purportedly at peace with the world, was engaged in any kind of warfare. (See: John A. Vasquez. "Conceptualizing War." In Nature of War: NW *Coursebook Academic Year 2002*. Compiled by Col(s) James Forsyth Jr., PhD, et al. Air Command and Staff College: Department of International Security and Military Studies. Maxwell, AFB, AL. Aug 2001, 1-2.)

[108] "Veteran Rocket Scientist Takes on New Mission." *Space News*, 8 April 2002, 46.

[109] "The Bush administration formally renounced support of the International Criminal Court yesterday, declaring that the world's first permanent war crimes tribunal would be an unchecked power, able to prosecute U.S. soldiers and their superiors." . . .based on fraudulent charges motivated by politics. Renouncement, however, "does not exempt

from prosecution Americans accused of war crimes committed after July 1, when the international court is set to convene in The Hague." The creation of the court followed ratification by 66 nations in Apr 2002 (including Britain, France, Germany and Canada), and so far 139 countries have signed. "Many of the United States' closest allies, including nearly the entire NATO alliance" as well as domestic supporters, opposed the administration's renouncement. (See: Peter Slevin, "U.S. Renounces Its Support Of New Tribunal For War Crimes." Washington Post, 7 May 2002, 1.)

[110] "NATO faced shortfalls in Information Warfare (IW) doctrine, concepts, and force structure. . . . As a result, NATO planners were less able to integrate the various IW capabilities [OPSEC, EW, CAN, CND, deception, PSYOPS, DCI, and physical destruction) into a coherent IW strategy that supported the air campaign, Moreover, NATO's overt [IW] efforts were not fully effective. . . IW in all its variations requires training in the doctrine, tactics, techniques and procedures that make IW weapons available to commanders at the strategic, operational, and tactical levels. (See: Headquarters United States Air Force. "The Air War Over Serbia: Aerospace Power in Operational ALLIED FORCE: Initial Report." In *Air and Space Operations, Coursebook Academic Year 2002*. Compiled by Col James Forsyth Jr., PhD, et al. Air Command and Staff College: Department of Joint Warfare Studies Department, Maxwell, AFB, AL. Aug 2001, 9.)

[111] The QDR, JV2020, NMS and Joint doctrine only recognize the term "Space Control."

[112] VAdm Bill Owens. *Lifting the Fog of War*. (New York: Farrar, Starus, and Giroux, 2000), 199.

[113] JP 3-13 also unfortunately states that CNA only "*may* be considered for development in Offensive Information Operations." See: JP 3-13, ix, II-3.)

[114] Lack of a common vernacular has stymied other government agencies, notably the FBI and CIA, which continues to focus on the tactical aspects of CNA, having no definitional/doctrinal framework to dissect the strategic nature of these attacks. Most analyses of attacks have focused on the tactical, verse strategic goals of attackers. Tactical support investigates attacks as singular incidents of identified vulnerabilities. "Examples of tactical support include analysis of (1) a computer virus delivery mechanism to issue immediate guidance on ways to prevent or mitigate damage related to an imminent threat or (2) a specific computer intrusion or set of intrusions to determine the perpetrator, motive, and method of attack." Strategic analysis looks at trends and analyzes singular threats as part of a broader whole, for example, as an attack against a national vulnerability. "Strategic analyses are intended to provide policymakers with information that they can use to anticipate and prepare for attacks, thereby diminishing [potential damage.]" Since its establishment, has focused its resources on the tactical. The GAO reports that strategic analyses has been lacking in that ". . . no generally accepted methodology for strategic analysis of cyber threats to the nation's infrastructures has been developed. Lacking are a standard terminology, a standard set of factors to consider, and established thresholds for determining the sophistication of attack techniques." The report cited the lack of staff in general, and experienced staff in particular. This is true not just in the DoD, but throughout the Government. The FBI in particular "lacks staff who are experienced in critical infrastructure operations and intelligence analysis." (See: General

Notes

Accounting Office. *"Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities"*, April 2001.) GAO-01-323, April 2001, 39.)

[115] Department of Defense. *Quadrennial Defense Review Report*. Washington DC: U.S. Government Printing Office, Sep 2001, 60.

[116] Antulio J. Echevarria II. "War, Politics, and RMA-the Legacy of Clausewitz." In *Nature of War: NW Coursebook Academic Year 2002*. Compiled by Col(s) James Forsyth Jr., PhD, et al. Air Command and Staff College: Department of International Security and Military Studies. Maxwell, AFB, AL. Aug 2001, 427.

[117] Echevarria II, "War, Politics, and RMA-the Legacy of Clausewitz," 427.

[118] "An extraordinarily sophisticated information technology (IT) infrastructure fuels America's economy and national security. Critical infrastructures, including telecommunications, energy, finance, transportation, water, and emergency services, form a bedrock upon which the success of all our endeavors -- economic, social, and military -depend. We must understand the vulnerabilities and interdependencies of our infrastructures, accept that such attacks know no international boundaries, and work to mitigate potential problems." (See: The White House. *A National Security Strategy for a Global Age*. Washington DC: Office of the White House, December 2000, 24.

[119] "The recent U.S. experience in Kosovo underscored the need for high-capacity, **interoperable communications systems that can rapidly transmit information over secure, jam-resistant datalinks** to support joint forces" (See: QDR, 45.)

[120] The White House. *A National Security Strategy for a Global Age*. Washington DC: Office of the White House, December 2000, 24.

[121] QDR, 50-54.

[122] Ibid.

[123] Ibid.

[124] Ibid.

[125] Ibid.

[126] Ibid.

[127] Ibid.

[128] Ibid.

[129] Ibid.

[130] Note the hierarchical arrangement in the figure. All Intelligence is comprised of information, in turn comprised of data derived from multiple sources, in the center. Leadership uses intelligence to command and control forces. The colors indicate the offensive and defensive counterparts (i.e. green to green, blue to blue, etc.) forming vertical angles. Consider the US is taking the offensive in the following vignette, moving counter-clockwise from 1200. Communications is used to command forces, and an adversary will try to deny US comm. The US will perform Suppression of Enemy Defenses and other Electronic Warfare (EW) techniques such as jamming. The adversary will counter with Defensive EW (such as their version of a HARM), or passive techniques like stealth. Advances in Information Technology allow the US to optimize its own OODA loop, while antiquated equipment will not exploit the state-of-the-art advantages, like speed and memory. Physical attack and physical defense, are obvious, but include OPSEC measures as well. Interoperability optimizes data exchange and accelerates the

Notes

US OODA loop, while stove-piped, mission-unique equipment slows down the OODA loop and may not even process the data. Interoperability provides for seamless C4ISR. Many systems even today, including the Prowler and AC-130 gunship, still cannot receive direct SatCom links. CNA and CND were discussed above. Psyops is included on both sides as it has an inherent offensive and defensive component. An adversary will execute their own Psyops campaign including counter-propaganda, spoofing, and information denial. Space Operations involve the force support and force enhancement benefits space superiority provides. Offensive counterspace involves actively denying, deceiving, disrupting, degrading, and/or destroying adversary space capability (SD5) predicated on sound surveillance. The adversary counters with passive and active means, including protection, maneuvering, and counter-attacking.

[131] US Department of Defense. *Joint Publication 3-13: Joint Doctrine for Information Operations*. Washington, DC., 9 October 1998, I-4.

[132] Department of Defense. Joint Publication 1-02: *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC., 12 April 2001 (as amended through 15 October 2001), 209.

[133] However, this would be inconceivable if the US adopted the Asian view of conflict.

[134] JP 3-13 also unfortunately states that CNA only "*may* be considered for development in Offensive Information Operations." See: JP 3-13, ix, II-3.)

[135] Maxwell's equations and Shannon's law (electromagnetic theory) do not change in different environments. Nor do Navier-Stokes and fluid dynamics equations--yet a submarine operates far differently than does a jet, or a ship for that matter. EW systems do not. They all have feeds, and antennas that channel incoming or out-going energy) either physically or electronically. The main difference is in EIRP.

[136] Secretary Rumsfeld is quoted as calling this "old think" which is pervasive in the higher echelons of the military, and forces the world to be "too regionalized," and unable to track threats from one continent to another, a poignant concern as globalization and globally available communication grows. (See: Harnden, Toby. "Rumsfeld Calls For End To Old Tactics Of War." *London Daily Telegraph*, 16 October 2001.

[137] Air Force Doctrine Document 2-2. *Space Operations*, 23 August 1998, 24. Note: several additional quotes are included in Appendix C.

[138] This concept is no different than say, a B-52 engaging in strategic conventional bombing, Close Air Support, or its nuclear mission. The B-52 is still just a delivery platform, analogous to the concept of the information.

[139] Includes active and passive radar, Synthetic Aperture radar, visible, multispectral, hyperspectral, and ultraspectral.

[140] "DoD must also undertake high-fidelity transformation exercises and experiments that address the growing challenge of **maintaining space control or defending against attacks** on the U.S. national **information infrastructure**." (See: QDR, 45).

[141] While kinetic-type weapons are sure to be developed given their heritage, their use will be restricted to all but the most dire circumstances. Potential adversaries are far more likely given the relative ease of detonating a nuclear warhead in space launched on a simple ballistic missile, than executing a sophisticated rendezvous in space against a

target actively employing escape and avoid maneuvers controlled by a global, redundant, and very sophisticated ground-based network. Thus, the use of the kinetic ASAT will become nearly as restricted as the use of nuclear weapons, and as such impotent, except in those cases where actual national survival is at stake.

[142] "[The Air Force is pursuing a "number of space control' initiatives [in 2002] . . . consistent with the growing emphasis on exploiting space to provide worldwide US forces with uninterrupted [C4ISR]. Systems are "believed to include jammers to block radio signals or lasers to blind the satellites' optical sensors." The USAF also intends to begin developing a small, mobile/transportable system to incapacitate satellite communications systems and a second system to counter surveillance and reconnaissance satellite systems." (See: Michael Sirak. "USAF Plans 'Space Control." *Jane's Defence Weekly*, 31 Oct 01, n.p. On-line. Internet, 20 December 2002. Available from http://131.84.1.68/Jan2002/e20020108roche.htm.

[143] John Grady. "Control of Space Crucial in Future Battles." *Army Link News*, 15 December 1997, n.p. On-line. Internet, 20 December 2002. Available from http://dtic.mil/armylink/news/Dec1997/a19971216space.html.

[144] Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (as amended through15 October 2001), 111.

[145] Gregory J. Rattray. *Strategic Warfare in Cyberspace*. (The MIT Press. Cambridge, MA), 66.

[146] JP 1-02, 209.

[147] Ibid, 216.

Chapter 4

Non-Materiel Solution: The Status Quo

Transformation is at the heart of this new strategic approach. The Department's leadership recognizes that continuing 'business as usual' within the Department is not a viable option given the new strategic era and the internal and external challenges facing the U.S. military. Without transformation, the U.S. military will not be prepared to meet emerging challenges.

—2001 Quadrennial Defense Review

We need to make the leap into the information age, which is the critical foundation of our transformation efforts.

—Secretary Rumsfeld

We're so conditioned as a people to think that a military campaign has to be cruise missiles and television images of airplanes dropping bombs and that's just false.

—Secretary Rumsfeld

Chapter 2 proved the threat is broad and enduring. Chapter 3 developed a new construct and definition for the requisite countermeasure and environment. The third section of a MNS analyzes the utility of using a "non-materiel solution"--that is, an *existing* construct to meet the threat. This chapter shows an existing construct will not suffice, and argues a new service instead is required to ensure unity of effort in *developing* (the role of a *service*) and then *employing* (the role of a *combatant command*) Information Operations (IO) weapons. To ensure objectivity, a precedent construct on service roles was used. In

"On Space Power Separatism," Shawn Rife convincingly argues the space mission area is not yet sufficiently mature whereby separation would optimize its military utility, and that merely being in a different environment does not necessitate a different service.[148] He states one must instead prove at least one of the following principles:

1. **Optimization:** "The requirements for that unique expertise are not being fulfilled within the current framework of organization, *or* the resources of that expertise are not being used properly."[149] (To aid the reader, tenets supporting this construct are labeled either **OP** or **OS**, for **O**ptimization **P**rimary, or **O**ptimization **S**econdary).
2. **Exclusivity:** "Only an *independent* space force can provide a capability that is considered vital to our national defense."[150] (Similarly, these tenets are labeled either **EP** or **ES**, for **E**xclusivity **P**rimary or **E**xclusivity **S**econdary).

Using his objective construct with respect to the I-Service, this chapter defends primary and secondary points (Tables 7 and 8) concluding the Air Force is ***appropriately*** focused on its critical mission of air superiority, but as such, lacks the span of control, acquisition system, and corporate will to champion increasing IO requirements. In addition to Rife's criteria, an independent Information Service meets the following two criteria: 1) it meets analogous requirements for a separate service. 2) it meets analogous tenants of Information Power as Mahan described for Seapower (Appendix D).

OP1: Focus on kinetic-based weapons. The USAF does have its priorities correct--maintaining and ensuring continued overwhelming air superiority. Unfortunately, the necessity to dominate that role is affecting its ability to objectively support its other core roles--space and information superiority. Top USAF officials are clear in their priorities. Gen Michael Ryan, CSAF from Oct 97 to Sep 01, clearly dictated his priorities noting the [fighter force is necessarily the Air Force's "primary focus."]151 Despite significant cost overruns and a countervailing Bomber review, the USAF's top two programs remain

Table 7: Optimization

<table>
<tr><td colspan="2">“The requirements for that unique expertise are not being fulfilled within the current framework of organization, <em>or</em> the resources of that expertise are not being used properly.”[152]</td></tr>
<tr><th>Primary</th><th>Secondary (in Appendix D)</th></tr>
<tr><td>OP1. The AF <b>appropriately</b> continues to promulgate kinetic-based weapons over space and/or information weapons</td><td>OS1. The QDR recognizes the need for, and calls for, significant transformation</td></tr>
<tr><td>OP2. The AF is becoming more reliant on weapon systems increasingly tied to Information while neglecting Information</td><td>OS2. Information Operations requires a new interpretation of Hague Convention and Geneva Convention statutes</td></tr>
<tr><td>OP3. The AF does not have the span of control to prosecute an air war, space war, and information war simultaneously at the strategic, operational, and tactical levels</td><td>OS3. AF senior leadership and PME billets are disproportionately allocated with respect to the USAF’s six core tenets</td></tr>
<tr><td>OP4. The DoD’s stagnant division of funding despite new mission areas and a new responsibility calculus fails to support its evolution</td><td>OS4. The Air Force has consistently been tied to dogma when it comes to evolutionary concepts</td></tr>
<tr><td>OP5. The Air Force itself remains fractured and tied to its core function of air superiority.</td><td></td></tr>
<tr><td>OP6. The DAL has concluded the AF is not providing the attendant structure required for a future air/space/I-Service</td><td></td></tr>
<tr><td>OP8. DOD has no single organization vested with the responsibility, authority and budget to acquire joint C4ISR systems, at the same time it is requiring increased interoperability.</td><td></td></tr>
</table>

Table 8: Uniqueness

<table>
<tr><td colspan="2">“Only an <em>independent</em> [Information] Force can provide a capability that is considered vital to our national defense.”[153]</td></tr>
<tr><th>Primary</th><th>Secondary (Appendix D)</th></tr>
<tr><td>EP1: The current military structure is antithetical with respect to the personnel, resources, and ties to industry</td><td>ES1. The other services are incapable of commanding an Information Service</td></tr>
<tr><td>EP2: The current DoD and AF acquisition systems are incompatible with the needs of an Information Service and in fact requires distinct acquisition procedures for Information Systems</td><td>ES2. The Information Service is far more pervasive across all IOPs than is the military IOP, and as such is fundamentally unique. (Proven in Ch 2).</td></tr>
</table>

the F-22 and the Joint Strike Fighter (JSF). In addition, Darleen Druyun, Principal Deputy to the Asst Secretary of the AF for Acquisition noted "Aircraft spending will account for nearly half of the Air Force's $155 billion acquisition budget over the next 5 years and will continue to be a top priority for the next 15 years."[154] This concentration on fighter aircraft affects not only information and space, but other *aircraft* as well, namely bombers, tankers, EW platforms, and some transports, as shown in Table 9, and detailed in Appendix D. The AF's evolution is likewise concentrated on the fighter infrastructure.

For example, with respect to bombers, Pentagon planners developed a bomber roadmap in response to 1999 Congressional budget hearings. Its findings were "inconsistent with the findings of the DoD's 1998 Long Range Air Power Panel [(LRAPP)]"[155] chaired by former CSAF Gen Larry Welch. The LRAPP found that "long-range air power is an increasingly important element of U.S. military capability" due to the loss of overseas bases, the advent of precision-guided conventional munitions and other factors."[156] The LRPAP made four key conclusions with respect to the bomber roadmap revolving around implausibly optimistic assumptions, neglect of the bomber force, and dangerously inadequate modernization plans[157.] The differences were so stark, several prominent Congressional members and retired GOs concluded it is the result of "bureaucratic politics within the service" wit respect to fighter pilot dominance.[158]

Table 9: Effect of Fighter Dominance On Other Airbreathing Platforms

Platform	**Main Concerns**
Transports	- The USAF is considering accelerating the procurement of C-130Js *only* to ensure the F-22 line (which shares the same assembly facility at Lockheed-Martin) is not impacted. This required significant restructuring of the C-130J program
Tankers	- Tanker fleet modernization has been so neglected the USAF will have to ***lease*** tankers from Boeing. Sen. Daniel Inouye (D-Hawaii), chairman of the Senate Appropriations Defense subcommittee, noted "[The KC-135Es] are ready to fall apart."[159] Yet tankers are critical to "thirsty" fighters that require significant refueling, and may be deprived of basing
Electronic Warfare	- There is spreading conviction among AF top officials (and independently ascertained by RAND) that it neglected its EW responsibilities to pursue stealth and that stealth has been oversold[160] - Premature retirement of the EF-111 Ravens - Congressional concern that "America's airborne EW forces are overworked and under-funded, [and] . . .no new air-frames have been produced in a decade"[161] - The SEAD mission is largely executed by a fleet of only 120 USN *Prowler*s for world-wide contingencies - After the loss of an F-117 in ODF that strayed outside its escort *Prowler*'s SEAD coverage, most stealth aircraft are required to fly with *Prowler* coverage

OP2: Increased reliance on weapon systems requiring Information Dominance .

The USAF's future force structure is increasingly and inextricably tied to manipulation of the Infosphere. While this fact may belie the idea that IO should be broken out into its own service, it actually underpins the span of control concern. Simply put, IO has become *so critical* and *so pervasive* to *all services* at the same time the talent pool has migrated to the more lucrative industrial sector, one service cannot, should not, and does not have the resources, to *alone* organize, train, and equip that element. Thus IO becomes the concern, the necessity and the province of every service.[162] Yet the DoD still must ensure Unity of Effort in that IO's key enabler is interoperability. A separate service is required. Even the USAF's true component of decisive force is tied to the EM spectrum in the form of UAVs, precision guide munitions (PGMs), Stealth, EW, and C4ISR for communication links to its future force. Yet the DoD is increasingly dependent on an infrastructure that is increasingly convoluted, weak, and vulnerable.[163] Table 10 highlights the AF's growing dependence on IO. Details are included in Appendix D.

Table 10: USAF's inreasing Dependence on Secure Information

Platform	Dependence	Vulnerability/Deficiency
UAVs/ UCAVs	- The QDR strongly endorsed UAVs noting "Efforts are underway to accelerate the procurement of …platforms including SIGINT payloads[164] - Based on performance during Operation Enduring Freedom, Global Hawk Block 10 versions were accelerated five years, and numbers increased 300%[165] - *Predator*s acquisition will increase 350%, from 7/year to 24/year.[166] - Manned platforms have an inherent vulnerability to creating a hostage situation or worse (e.g. EP-3E crew downed in 2001, Maj Rudolph Anderson during the Cuban Missile Crisis, and Gary Powers during the Cold War, etc.) - UAVs are being used like whiskers, tied to AC-130 gunships feeding live video to extend the venerable gunship's range - DARPA is said to be experimenting with UAV *helicopters*	- Comm links - Bandwidth - GPS accuracy (a particular concern with UCAVs) - Interoperability
PGMs	- Rapid transformation of majority of USAF munitions including kit-modified JDAM and JASSM air-ground missiles (Example: 73% of the munitions in OEF are PGMs[167]) - The QDR likewise noted the DoD "will also increase procurement of precision weapons."[168] - Precision engagement is core tenet of JV2020 - Precision strike is core tenet of USAF doctrine	- GPS vulnerability - Comm links to enroute aircraft - Spoofing - Meaconing - Intelligence key (e.g. Chinese Embassy incident) - Real-time Sensor to Shooter requirements

Table 10 (Cont.): USAF's inreasing Dependence on Secure Information

Platform	Dependence	Vulnerability/Deficiency
Stealth	- The necessity for stealth as IADS capability proliferates and improves[169] - Stealth fighters and bombers - Stealthy attributes built into all new air platform designs (e.g. F-22, JSF), including UAVs/UCAVs - Stealth attributes are also being incorporated into aircraft carriers, submarines, and tanks and helicopters - A net increase of 32% in R&D related to stealth and other enabling technologies - "Combined-arms" stealth operations are being improved to the point that missions can be shifted from night-only using other planes to conceal the stealth aircraft within their own radar signature[170]	- Stealth has been compromised (e.g. F-117 lost during ODF)[171] - Historical over-reliance on stealth to detriment of SEAD - New advances in computational power may employ a passive cell phone net to render stealth obsolete - Stealth aircraft are now routinely escorted by EA-6Bs for SEAD[172] - Cost (B-2 ~$500M, Stealthy UAV estimated to cost $200M/each[173]).
C4ISR	- Defined as a critical enabler in the NSS, NMS, QDR and assigned primacy in JV2020[174] - Smaller footprint tied to a leaner, more rapidly deployable force[175] - A growing reliance on Reachback - A growing reliance on SOF executing "covert deep insertions over great distances" and the corresponding need for enhanced C4ISR"[176] - Increased reliance on persistent ISR[177] - Increased reliance on jam-resistant, high capacity communications[178]	- DoD SatCom is vulnerable - Commercial SATCOM are highly vulnerable - Adhoc interoperability - DoD Space-based ISR assets are vulnerable - Little HUMINT assets in most trouble countries

<u>OP3: The Air Force does not have the requisite span of control.</u> The nature of the international environment--one of increasing globalization, technology, singular military dominance, and destabilization along cultural and ethical lines--is posing a problem no *single* service is capable of optimally managing. By way of example, in a span of only a few years, Table 11 demonstrates the incredible extent to which the USAF's responsibilities have expanded:

Table 11: USAF Increasing Roles

USAF Core Competency	Magnitude of Change	Details
- Air and Space Superiority **- Information Dominance** **- Precision Engagement**	New	- The Air Force designated the lead role for space (17 years after AFSPACECOM established)
- Air and Space Superiority **- Information Dominance**	Increased Emphasis	- The Space Broad Area Review declared space situational awareness was the key space priority and designated the Air Force as lead. However, the SBIRs program is in disarray, several surveillance missions have been shunted to the BMDO office, and the ground-space surveillance system is managed b the USN[179]
- Information Dominance	New	- With the 1 Oct 2000 UCP vesting the CNA and CND missions to USSPACECOM, and their subsequent delegation, the increased reliance on USSPACECOM to include ". . . serving as the military lead for computer network defense (CND) and, effective 1 October 2000, computer network attack (CNA), to include advocating the CND and CNA requirements of all CINCs, conducting CND and CNA operations, planning and developing national requirements for CND and CNA, and supporting other CINCs for CND and CNA."[180]
Air and Space Superiority	New	- An increasing emphasis on space control - Rumsfeld's transformation memo of 18 Oct 2000 called for a rapid and substantial increase in space control efforts - Pervasive emphasis throughout the QDR - "Defense Secretary Donald Rumsfeld announced in May that the Air Force would be the lead service for organizing, equipping and training personnel for both offensive and defensive space operations--including planning and acquiring space based equipment."[181]
- Air and Space Superiority **- Precision Engagement**	Increased Emphasis	- An increasing role in UAV/UCAV development and acceleration of acquisition

Table 11 (Cont.): USAF Increasing Roles

USAF Core Competency	Magnitude of Change	Details
- All	Increased Emphasis	- An increasing role in MOOTW, to include strategic bombing missions to the exclusion of ground forces to limit casualties. This was seen in **Desert Storm**, ODF and to a great extent in OEF with the Air Force delivering 80% of the ordnance - An increasingly dominant role in coercive force
Air and Space Superiority	New	- A new role in Homeland Defense after 9/11. This is supported by an increase of $1.2B in the defense budget for Combat Air Patrols (CAP) and the Feb 2002 acknowledgment CAP is logistically unsupportable. (The CAP "is a considerable strain" not only because the USAF is keeping "one-sixth of its reserve component on active duty 9but because] the US maintains only four squadrons of dedicated sir defense interceptor aircraft, or about 75 …planes."[182] The Brookings Institute, in "Protecting the American Homeland" cites airborne assets as "the linchpin of homeland protection" with a cost of $30B.[183]

By recognizing that space is a subset of IO, and by designating a new service as the lead for information, the USAF will best be able to concentrate on its core mission area--air superiority.[184] The Air Force has long argued that it relies on its space systems to do its mission effectively.[185] That it depends on space for its role is no different than its reliance on the Navy for suppressive cruise missile attacks, SEAD, and for transport,[186] the Army to secure ground, provide the fine tuning of coercive force during a bombing campaign the USAF cannot provide, and its mutual support against C2 and IADS. All services depend on space,[187] and all depend on information, and that dependence is growing promulgated by both leadership and technology (Fig. 12). A Combatant Command fights as a team--the administrative role--that *recruit, organize, train, and equip* role--however, is needlessly suffering due to politics and interservice rivalries, and sub-optimizing the DoD's ability to equip that team.

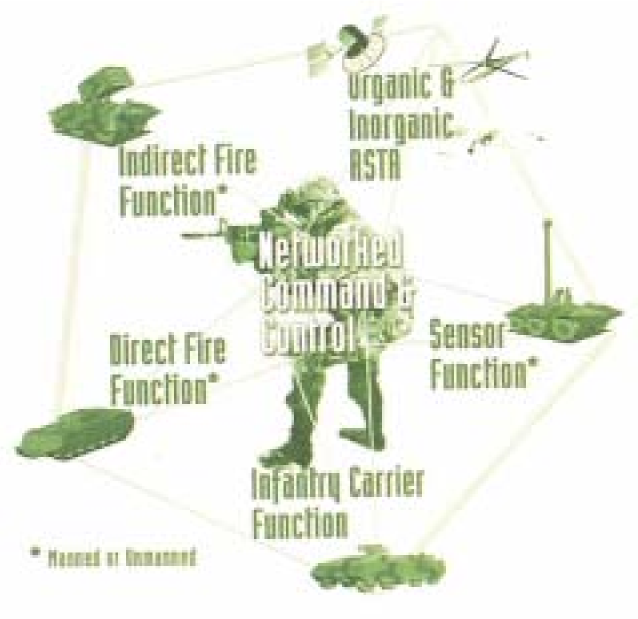


Figure 12: The US Army is becoming dependent on real-time C4ISR

OP4: <u>The DoD's stagnant division of funding fails to support its evolution.</u> While the USAF is taking on these additional responsibilities, its budget share remains stagnant. The use of airpower, space superiority and IO are all sharply increasing. The AF budget cannot remain stagnant and simply pit these mission areas against one another in a zero-sum game--space and IO will always lose out to kinetic forces given the mind-set of current leadership. The more pressing concern is the stagnant division of funding not within the AF, but within the DoD. The decade following the establishment of the AF as a separate service reflected a budget re-distribution commensurate with its birth

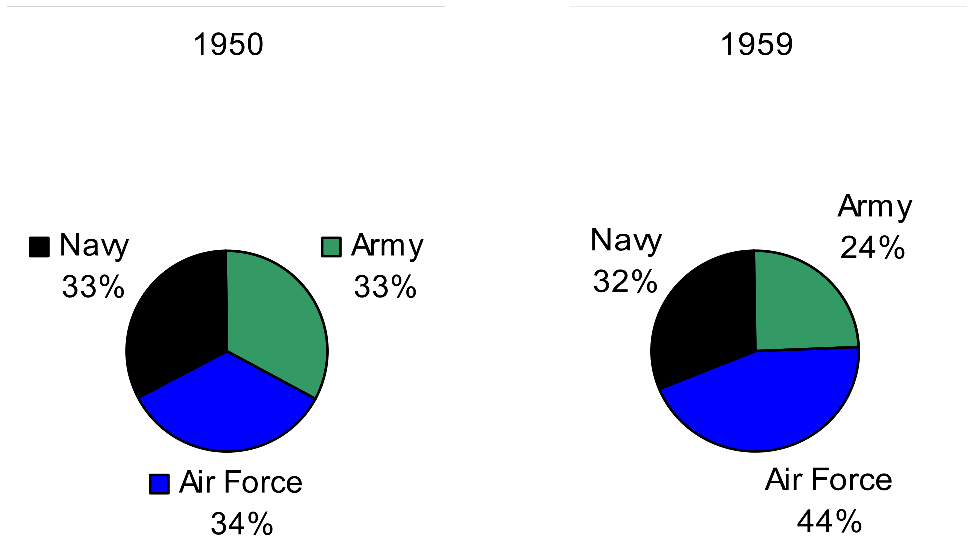
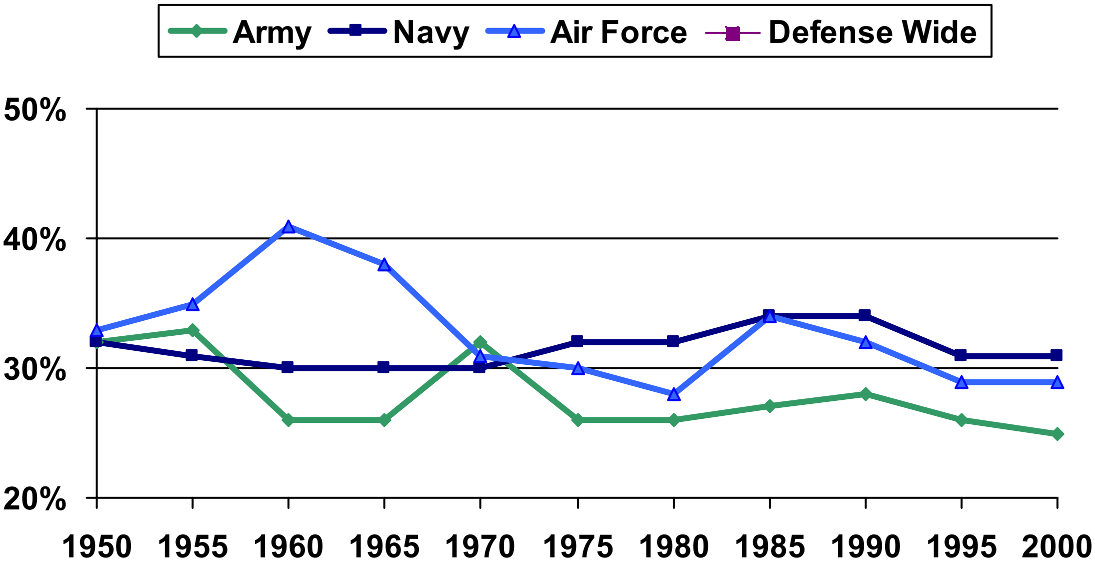


Figure 13: Nominal Redistribution Necessitated by Changing Roles

and the growing preeminence of the nuclear forces, as shown in Fig. 13. That pales in comparison to the budget distribution since 1960 which remains latent despite the many changes the forces have endured, and the increasing role of the USAF.[188] Despite significant changes, the Air Force's budget relative to the other services did not appreciably change. Fig. 14 shows a consistent ratio of 28:31:33 between the Army, Navy and USAF with little standard deviation--3.3%, 1.7%, 4.5%, respectively.[189]



Source: SAF/XP. DoD Budget Outlays.

Figure 14: Four Decades of Stagnant Funding Distribution

OP5: <u>The Air Force itself remains fractured</u>. In "The Icarus Syndrome," Carl Builder describes his concerns with the deteriorating Air Force by analogizing the state of the service to that of Icarus, the doomed son of Daedelus who flew too close to the sun.[190] Builder's analogy is on target, if somewhat incomplete. Icarus flew too close to the sun because he began to think of himself as a *god*, and soared toward Olympus to join the "other" Olympians. He lost his perspective as a fallible creature with limitations and the reality of the environment (in this case *the sun*, in the USAF's case the anarchistic struggle for balance of power as a function of structural realism), destroyed him. So too has the Air Force lost its way, spurred on its by its own press and spiraling onward on a desperate "Search for Douhet" to legitimize itself with respect to its older siblings/services, while protecting its younger siblings--space and information, from aligning with them. Builder correctly surfaces the true danger to the USAF--that it is wed to the concept of airplanes (and manned, fighter airplanes at that), vice the concepts of airpower--namely the speed, versatility and perspective afforded by airpower.

Several independent studies by Drs. Earl Walker and Arnold Kanter, and by LtCol Franklin Margiotta and James Smith, confirm Builder's thesis that this misalignment between true and articulated goals causes significant cohesion problems in the USAF. As detailed in Appendix D, all agree the USAF is the least cohesive of all the services, the main cause being the "caste" system between "flyers" and support personnel exacerbated by a growing technological divide. This technology gap, with the advent of the ubiquity of the Infosphere, will only further fractionate the force along the same technological line, and minimal/slow transformation will only worsen the growing rift. Further, that rift is "firmly rooted in Air Force culture, subcultures, and organizational dynamics within the diverse, complex entity that is today's USAF."[191] Dr. Walker further asserts that

> "**true** organizational change requires a **cultural transformation**--not simply accommodation and incremental modification but changed organizational output in terms of **structure**, professional incentives, and changed professional behaviors [emphasis added]."[192]

OP6: DAL has concluded the USAF is not providing the attendant structure.

MGen (ret) Chuck Link is heading the Developing Aerospace Leaders (DAL)[193] program, being conducted by RAND.[194] RAND determined that even though

> "[m]ultiple, significant changes, past, current, and pending are challenging the global society, we were building a GO force that was specialized, and that the overall GO experience base is relatively narrow. [The study also supported Builder's findings noting] the AF has become a confederation of tribes, and while arguably has no match . . .*tribalism* had precluded *nationalism*, that overarching *institutional* mindset. These tribes had allegiances toward traditional tribal functions, working to advance the interests of tribes. [Also] in that "career paths are stove-piped, the greatest rewards is staying on a straight path with the same tribe[emphasis added.]"[195]

The calculus of the top USAF leadership supports RAND's findings. Current and projected AF leadership confirms these conclusions, as noted in OP7. In addition, space is fragmented within its own AOR.[196] MGen (S) Michael Hamel, Director, Space Operations and Integration, noted "One of the key findings of the space commission was that there is serious fragmentation in leadership across the national security space community," emphasizing the corrective changes the new DUSD Space, Peter Teets, is taking.[197]

OP7. AF leadership/PME billets are disproportionately allocated. Synthesizing 1997 data[198] in Tables 12 and 13 show that although only 18% of the USAF were pilots, 70% of the senior leadership were pilots, a 4:1 ratio. And although 82% of the force remains in non-rated operations or in support billets, they are commanded by less than 25% of its corresponding leadership. The author is not trying to overstate the fact that "it's a pilot's Air Force," or that such is a problem--the USAF's key mission area *is* **air superiority--**pilots should be in charge. But the Air Force must recognize it may not have GO's with the requisite breadth of experience in space operations and IO to effectively exploit--and just as importantly *procure*--these new weapons, which comprise its other core capabilities. The problem, echoed by the Center for Strategic and Budgetary Assessments, is that "of the top USAF leadership only one has a significant background in bombers," in an age where the USAF "increasingly is being used for long-range airstrikes."[199] The report targeted its criticism at the USAF's leadership structure, emphasizing "Personnel choices lead to procurement choices." [200] And procurement is the responsibility of a **service**, not a combatant commander.

Table 12: General Officer Statistics

Rank	Total # of GOs	Fighter Pilot	Bomber Pilot	Airlift/Tanker Pilot	Total GO Pilots	Navigators	Non-Rated
O-10	11	9	2	0	11	0	0
O-9	36	18	4	3	25	0	11
Total GO O-9 to O-10	47	27	6	3	36	0	11
Percentage		**57.4%**	12.8%	6.4%	**76.6%**	0.0%	23.4%
O-8	78	39	6	12	57	1	20
O-7	122	44	11	23	78	3	41
Total GO O-7 to O-8	200	83	17	35	135	4	61
Percentage		**41.5%**	8.5%	17.5%	**67.5%**	2.0%	30.5%
Percentage of all GO's	247	**44.5%**	9.3%	15.4%	**69.2%**	1.6%	29.1%
Total GO's with Pilot Background in 1997	247	110	23	38	171	4	72

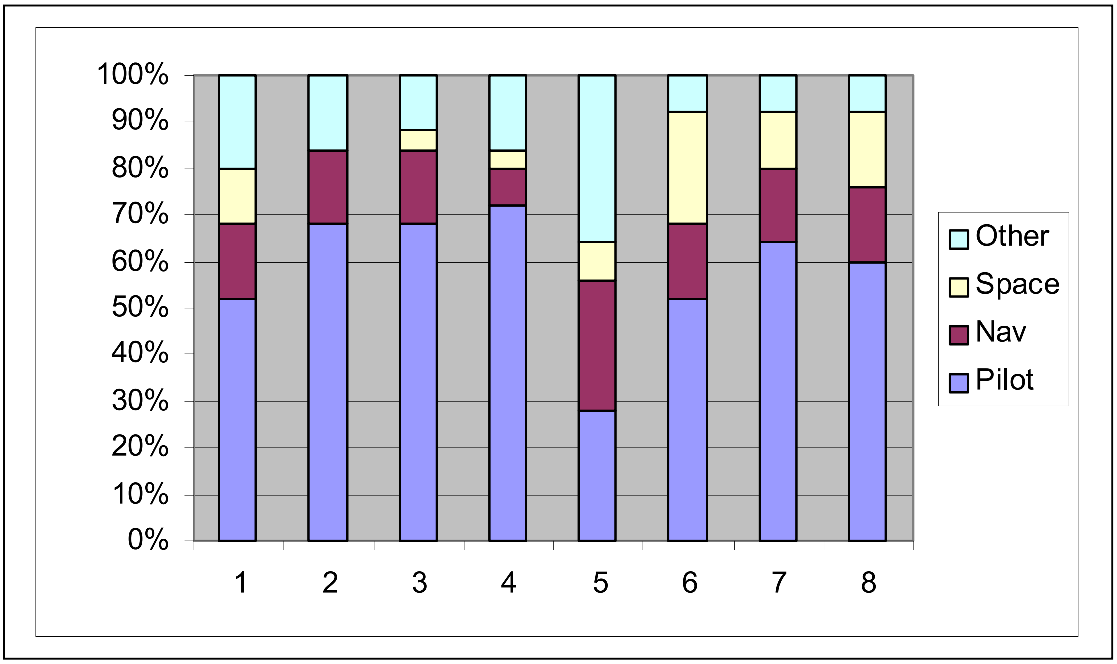
Table 13: . . . vs. AF Population Statistics

Total GO's with Pilot Background in 2001	272
Total Officers in 1997	73,710
Total Officers in 2001	67,373
Total Pilots in 1997	13,410
Total Pilots in 2001	11,178
Percentage of Force that were Pilots in 1997	18.2%
Percentage of Force that were Pilots in 2001	16.6%
Drop in # Officers Btwn 1997 and 2001	8.6%
Drop in # Pilots Btwn 1997 and 2001	16.6%

Because this calculus is a snapshot in time, and the Information Age only really hit its stride 12 years ago, it is prudent to postulate which officers will be leading the USAF in this new century and/or writing its doctrine. The trends are likewise disturbing. AU's School of Advanced Airpower Studies (SAAS) is an elite college whose mission is

> "to educate strategists in the art and science of aerospace warfare, thus enhancing the USAF's capacity to defend the United States through the control and exploitation of air and space."[201]

But again, SAAS is heavily attended by pilots (the majority coming from fighter airframes), with disproportionate numbers of space, information, communication, logistics, and other disciplines, as shown in Table 15. Col Stephen Chiabotti, the commandant at SAAS, while noting the apparent disparity, likewise felt the point of this research was diametrically opposed to the core needs of the force and thus its fundamental thesis flawed. He emphasized instead that fighter pilots will and should run the Air Force, and that "we need to change the fighter pilot, not the Air Force." He likewise noted that simply quoting statistics does not tell an accurate story in that the school ensures *all* its students research areas outside their core AFSCs, and thus graduates masters of the airpower theory vice simply "a better educated pilot."



Source: School of Advanced Airpower Studies Briefing, Col Stephen Chiabotti.

Figure 15: SAAS AFSC Demographics

OP8: DOD does not promulgate Unity of Action in acquiring C4ISR systems.

No other system--aircraft, satellite, ships, or artillery--connect the component forces to one another as does C4ISR. C4ISR is the one system that must be immediately interoperable[202] upon deployment and the one system that allows joint force commanders to command, control, and communicate with tailored force packages comprised of distinct service and/or functional components to inculcate unity of effort. The QDR was clear in its wording with respect to C4ISR--"***develop*** an interoperable, joint C4ISR architecture and capability [emphasis added]."[203] It did not state "*continue* to develop joint C4ISR", or "*improve* C4ISR"--the SecDef was clear in his evaluation--**the DoD has not yet made the progress it needs to in this vital area**. While the DoD has progressed substantially since Desert Storm when Navy aircraft physically transported the Air Tasking Order (ATO) from the JFACC's AOC to its fleet, the DoD has not progressed to the requisite level of interoperability. Recent military operations confirmed the lack of progress.

USN Navy *Prowler*s, the DoD's only SEAD aircraft still lacks SatCom capability and only AC-130 gunships are capable of receiving real-time *Predator* feeds. Other strike aircraft still require vulnerable ground controllers to designate targets.

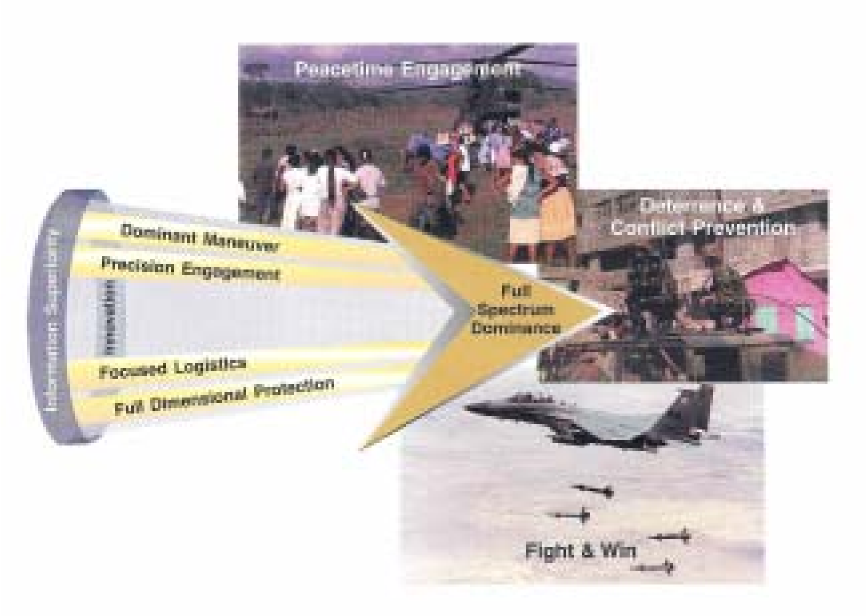


Figure 16: Information Superiority is Critical Enabler to Future Force Capability

It's not the *number* of ISR assets, but the fact they are not interoperable which is limiting their potential.

> "Top Pentagon and defense industry officials contend that nearly all the intelligence and targeting information they need is already being collected. The problem is that the data usually stays with the platform that collects it . . . [while] . . . fighting units are desperate for [it]. . . . The solution is not to buy more ships, aircraft and vehicles to collect more data, but to make existing information available on a wide-distribution communications network."[204]

General Gregory Martin, Commander of U.S. Air Forces, Europe agrees, noting:

> ". ..'Our ISR posture as a nation is woefully short of the needs, from space to HUMINT, [in] every bit of [ISR] capabilities.' While emphasizing US ISR assets are still superior to those of any other country . . .**'we have to have a more connective** and more persistent intelligence network.' He noted that the challenge for the U.S., however, is not just to get more sensors and more ISR assets, **but to connect those sensors** that the

> services already have [noting] **many of the current ISR assets are not interoperable** [emphasis added.]."[205]

In addition, every major acquisition program must meet a single common criterion: Interoperability. Interoperability is achieved through IT and a system cannot proceed through initial acquisition stages[206] until it meets the criteria of the Clinger-Cohen Act, and has vetted its C4I plan with J-6. **Every program.** Yet the DoD has no single agency responsible for the vision, development, acquisition, management and verification of all C4ISR programs.[207] Those responsibilities are split out between the services, and in fact, within the services, and among OSD offices. This violates Unity of Effort. Unity of effort is not a concept isolated to the battlefield--it is achieved anytime a group of actors with different standards, agendas, and perspectives coalesce to drive toward a single focus. If a new service is not the answer, certainly, a joint C4ISR program office is.

This interoperability problem will only grow, unless a concerted effort is undertaken to force interoperability *a priori* into new systems. That must be done by a single command, that has joint responsibility, joint funding, and is overseen by a joint board. That service can optimize the myriad intelligence, information-in-warfare, information operations, and both offensive and defensive efforts. As this I-service improves its offensive capabilities, it likewise exposes its analogous vulnerabilities and realizes its necessary defensive posture. This symbiotic relationship is critical in that IO weapons are inherently offensive weapons.[208] Such synergy is possible if the systems that comprise and operate within the Infosphere are consolidated and a single agency and a single individual is responsible and accountable for their integration and interoperability.

This synergy is not happening in the program offices of the individual services or at the DoD level.[209] For example, the USAF's premiere air battle planning system, the

Theater Battle Management Core System (TBMCS), has no provisions to develop IO targets, and few capabilities related to space. Yet ACC, TBMCS's end-user, was assigned the IO mission.[210] Space assets and CNA/CND targets meanwhile will be C2'd by the NORAD/USSPACECOM Warfighting Support System (N/UWSS)[211] controlled by USSPACECOM. As such, USSPACECOM is providing troops to prosecute only a part of the IO, and a part of the campaign *only the Air Force* believes is IO, in that joint doctrine has not considered the IO vs. CAN/CND issue. Meanwhile, the rest of the IO campaign is being executed by ACC, which does not have the C2 planning system to prosecute the IO (or asymmetric) target set. AC2ISRC acknowledged the significance of the disconnect. In fact, there are literally hundreds of different C4I systems being developed by the three service C2 centers.[212] A single service responsible for DoD-wide C4ISR would minimize the overlap and is in line with the metered transformation called for in the QDR. Col Chiabotti, a USAF command pilot with several tours in acquisition program offices, vehemently disagrees. He instead believes a separate I-Service would exacerbate the current acquisition problem by further isolating the warrior from the acquisition office, which he believes is not incentivized to meet operational requirements.

EP1: Current military structure will not support the necessary I-Service. An I-Service is antithetical with respect to the current DoD in three regards centered on the issue of lethality: 1) Individual capacity 2) Speed, and 3) Discipline. In terms of individual capacity, a soldier, sailor, and airman cannot alone disable significant adversary assets--information operators can--and have, and can do it thousands of miles from the battlefield. In addition, their payloads are delivered at the speed of light, and can render systems temporarily or permanently disabled within seconds. In terms of discipline, IO requires a class of non-conformity and dynamic thought antithetical to military culture. That requisite military hierarchy and demand for conformity has been proven time and time again to hinder innovation, a concern which pervades the QDR. Creating a service as a sub-element of the existing force would only engender these same constraints. Creativity is impeded when too much emphasis is placed on the following elements:

Table 14: Inherent Impediments to Creativity

Negative Element	Kendall's description	Potential Conflict Between Current Military Structure and IO
Specialization	"… the military tends to go to the extreme and isolates officers from the 'big picture.'"[213]	DAL shows the Air Force has not developed the requisite breadth and depth in the required set of leaders.
Departmentalization	"…can limit channels of information. An empirical study concluded that departmental organizations create many managers who can detect and solve problems relating only to their specific jobs."[214]	Again, the military organization, with its necessary hierarchal structure is highly departmentalized.
Structuralization	"A military structure is needed, but it can exert great pressure on individuals to perform, thus reducing creativity. Even if the environment is not truly conformist, it can still be detrimental if the officer feels that the surroundings warrant conformance. Thus, the officer spends a lot of time trying to conform. Conformity can alienate the creative individual from the group and, in so doing, limit information channels."[215]	The military structure is necessarily rigid. An IO unit must be more horizontal to attract and retain the brightest.

<u>EP2: The I-Service is incompatible with DoD and USAF acquisition procedures.</u> Submarines, aircraft carriers, tanks, rations, satellites, all aircraft--even manpower and toiletries--are all governed by the same procedures when acquiring systems, items, and personnel services. IT systems, however, are **inherently different**, requiring **different thresholds, oversight, approval mechanisms, and even separate criteria**, as detailed in Table 15.

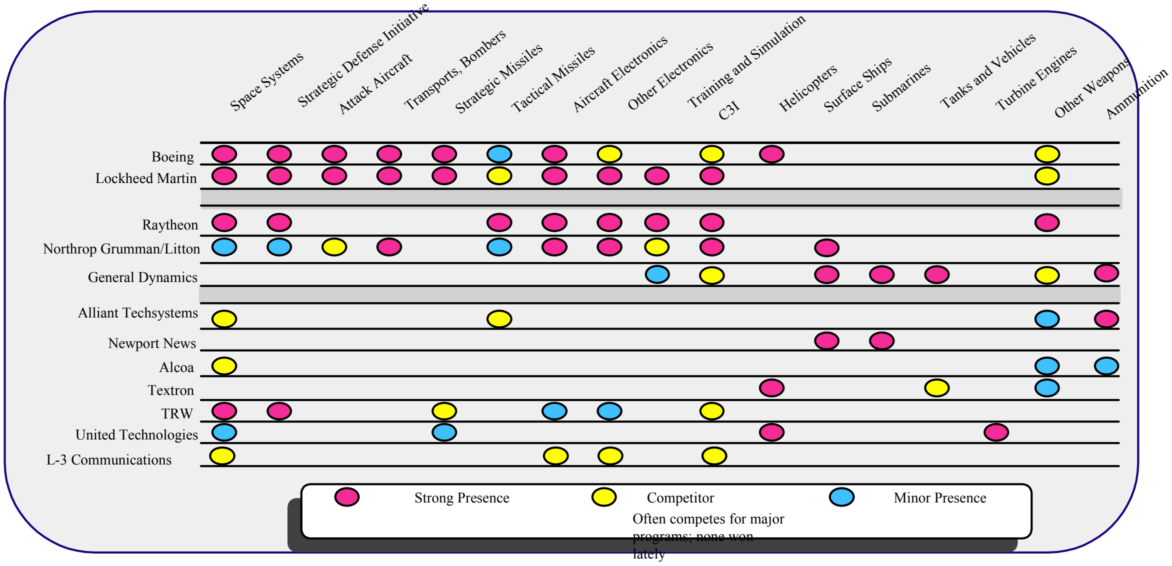
Table 15: Revealing Differences between Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAISs)

Criteria	MDAP	MAIS
Designation	Scaleable from ACAT ID/C to ACAT IV[216]	All are ACAT I
Funding Thresholds[217]	- $365**M** RDT&E - $2.19**B** Procurement	- $378**M** Life-Cycle Cost - $126**M** Total Program Cost
Oversight	Lead Service (joint) or Service	Chief Information Officer (CIO)
Milestone Decision Authority (MDA)	USD (AT&L)	CIO (ASD/C3I)
Funding Oversight	Cost Analysis Improvement Group	None required
Distinct Controls	- IT KPP slaved to IT maturity - Selected Acquisition Report - Unit Cost Breaches - Beyond Low-Rate Initial Production Report - Live Fire Test & Evaluation Report	- IT KPP architecturally defined - Compliance with Clinger-Cohen Act of 1996 - J-6 C4I Interoperability review required

Source: AP-772: Acquisition Oversight, Review, and Decision Authority, DSMC[218]

Instructors at the Defense Systems Management College,[219] speculated that the division was due in part to DoD's inability to "to think outside of the box, [in that C4ISR systems] are a wholly different animal that do not play by the rules."[220] For example, overly restricted classification guidelines remain a significant hindrance to acquiring systems. Separate organizations feed this classification problem--a single organization would be instrumental in breaking down unnecessary barriers since it would hold the majority of security billets. In addition, as new technology becomes outdated, those once highly classified systems will eventually become mainstream and security downgraded. The same standard will greatly ease the transition from black-world to white-world. IT programs are also unique in one other regard--**every** major weapon acquisition must have an interoperability KPP--the only common KPP which pervades every acquisition.

In addition, the typical DoD acquisition program office[221] and culture is incompatible with the needs of the I-Service. Gen. Martin and Gen Lord likewise note that "Air Force C^2ISR networks include not only technical systems **but also personnel and processes** . . . Since Air Force C^2ISR systems that collect and distribute data are mostly operated by 'stovepipe' organizations, **getting the people involved to think in new ways** will be the key to success [emphasis added]."[222] Simply birthing it under the USAF for example, would only duplicate the flawed structure used in its space and C2 acquisition centers, the latter of which has recently come under heavy criticism by both USAF Secretary Roche and Undersecretary/NRO Director Teets.[223] In addition, the traditional contractor base--given the significant downsizing the defense industry has undergone since the mid-1980s--is ill-prepared to take on this new challenge. While smaller, stronger, and more diversified, its traditional strengths are not Information-based. The IT talent pool lies in commercial industry.[224] Yet 70% of the IT companies will not do business with the DoD because of DoD's antiquated acquisition practices and its lack of respect for intellectual property rights,[225] the very lifeblood of IT companies, where dual-use technology is the norm vice a bureaucratic metric. MIT strategist Greg Rafferty agreed noting the leading status of the IT industry will "make government control …very difficult."[226]



	Space Systems	Strategic Defense Initiative	Attack Aircraft	Transports, Bombers	Strategic Missiles	Tactical Missiles	Aircraft Electronics	Other Electronics	Training and Simulation	C3I	Helicopters	Surface Ships	Submarines	Tanks and Vehicles	Turbine Engines	Other Weapons	Ammunition
Boeing	🔴	🔴	🔴	🔴	🔴	🔵	🔴	🟡		🟡	🔴					🟡	
Lockheed Martin	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔴	🔴						🟡	
Raytheon	🔴	🔴				🔴	🔴	🔴	🔴	🔴						🔴	
Northrop Grumman/Litton	🔵	🔵	🟡	🔴		🔵	🔴	🔴	🟡	🔴		🔴					
General Dynamics									🔵	🟡		🔴	🔴	🔴		🟡	🔴
Alliant Techsystems	🟡					🟡										🔵	🔴
Newport News												🔴	🔴				
Alcoa	🟡															🔵	🔵
Textron											🔴			🟡		🔵	
TRW	🔴	🔴			🟡		🔵	🔵		🟡							
United Technologies	🔵				🔵						🔴				🔴		
L-3 Communications	🟡						🟡	🟡		🟡							

🔴 Strong Presence 🟡 Competitor Often competes for major programs; none won lately 🔵 Minor Presence

Figure 17: Traditional DoD Industry Has Broadened in Past 15 Years

<u>An I-Service meets the requirements for a separate service.</u> Analogizing a new service against its sister services must not only use the same structure that frames the other services (e.g. role, mission, core functions), but must ensure it is predicated on a threat that is not or cannot be mitigated by the other services, must be uniquely defined, and must be realistic in scope. For example, an independent space force does not meet these criteria in that it lacks a realistic force application capability. Table 16 summarizes this process and concludes an independent I-Service does indeed meet analogous criteria.

Table 16: Information Service Basic Precepts

Factor/ Service	USA	USN[227]	USMC	USAF	Info
AOR	Land	Sea	Littoral	Air	InfoSphere
Conducts	Land Operations	Sea Operations	Amphibious Operations	Air Operations	Information Operations
Dominates	Land	Sea/ Sub-surface	Littoral	Air	Infosphere (inc. space)
Needs	Land Superiority	Sea Superiority	Littoral Superiority	Air Superiority	Info Superiority
Ultimately wants	Land Supremacy	Sea Supremacy	Littoral Supremacy	Air Supremacy	Information Supremacy
In War, it projects	Land Power	Sea Power	Amphibious Power	Air Power	Info Power
Executes the	Land War	Sea War	Littoral War	Air War	Info War
Directive	10 U.S.C. 3062b	10 U.S.C. 5062	10 U.S.C. 5063	10 U.S.C. 8062c	TBD
Shall be organized, trained, and equipped to . . .	primarily for prompt and sustained combat incident to operations on land. It is responsible for the preparation of land forces necessary for the effective prosecution of war [228]	primarily for prompt and sustained combat incident to operations at sea. It is responsible for the preparation of naval forces necessary for the effective prosecution of war, except as otherwise assigned, and is generally responsible for naval reconnaissance, antisubmarine warfare, and protection of shipping. [229]	to provide Fleet Marine forces of combined arms, together with supporting air components, for service with the fleet in the seizure or defense of advanced naval bases and for the conduct of such land operations as may be essential to the prosecution of a naval campaign. [230]	primarily for prompt and sustained offensive and defensive air operations.[231]	Primarily for continuous defensive operations to protect the national information infrastructure and for prompt and sustained offensive information operations
Includes	land combat and service forces and any organic aviation and water transport assigned.	in general, naval combat and service forces and such aviation as may be organic therein.		aviation forces, both combat and service, not otherwise assigned.	

Table 16 (Cont.): Information Service Basic Precepts

Factor/ Service	USA	USN[232]	USMC	USAF	Info
Responsible for	the preparation of land forces necessary for the effective prosecution of war and military operations short of war	the preparation of Navy and Marine Corps forces necessary for the effective prosecution of war and military operations short of war . . .		the preparation of the air forces necessary for the effective prosecution of war and military operations short of war, except as otherwise assigned and, in accordance with integrated joint mobilization plans, for the expansion of the peacetime components of the Air Force to meet the needs of war.	the preparation of the Information Services necessary for the continuous vigilance required to protect the US information infrastructure and effective prosecution of war and military operations short of war, except as otherwise assigned and, in accordance with integrated joint mobilization plans, for the expansion of the peacetime components of the Information Service to meet the needs of effective prosecution of any national instrument of power.
Primary Function	To organize, train, and equip forces for the conduct of prompt and sustained combat operations on land--specifically, forces to defeat enemy land forces and to seize, occupy, and defend land areas.	To organize, train, equip and provide Navy and Marine Corps forces for the conduct of prompt and sustained combat incident to operations at sea, including operations of sea-based aircraft and land-based naval air components--specifically, forces to seek out and destroy enemy naval forces and to suppress enemy sea commerce, to gain and maintain general naval supremacy, to control vital sea areas and to protect vital sea lines of communication, to establish and maintain local superiority (including air) in an area of naval operations, to seize and defend advanced naval bases, and to conduct such land, air, and space operations as may be essential to the prosecution of a naval campaign.		To organize/ train/equip, and provide forces for the conduct of prompt and sustained combat operations in the air--specifically, forces to defend the United States against air attack in accordance with doctrines established by the JCS, gain and maintain general air supremacy, defeat enemy air forces, conduct space operations, control vital air areas, and establish local air superiority except as otherwise assigned n.	to maintain, train, and equip combat-ready forces to Preserve the peace and security and provide for the defense of the United States by deterring or defeating enemy aggression through control and exploitation of the InfoSphere

Summary. This chapter arguably defended that the existing DoD construct or a modified DoD construct (i.e. the non-materiel solution) would be sub-optimal in acquiring and prosecuting information operations, upon which all services and facets of American society depend. Specifically, it non-pejoratively challenged the Air Force's ability to manage the growing area as a function of limited span of control, air-centric doctrine and leadership calculus, a history of dogmatic thinking, and lack of true budgetary evolution within the DoD. Particularly for this last reason, evolution is required at a level unprecedented since the USAF broke from its Army tethers 55 years ago. Appendix A provides one strawman representation of one way to realize that evolution, and in particular, the transformation required in the QDR.

.

Notes

[148] The USN employs assets on land, sea, sub-surface, space, and information--two more media than does the USAF.

[149] Maj Shawn P. Rife. "On Space Power Separatism." In *Airpower Studies: AP Coursebook Academic Year 2002*. Compiled by LtCol Micheal Fiedler, Phd, et al. Air Command and Staff College: Department of International Security and Military Studies. Maxwell, AFB, AL. Aug 2001, 393.

[150] Ibid.

[151] General Ryan said during the interview wrt to two question on modernization and retention: "It is important to maintain the "air" side of our air and space force. The group that executes that mission, our rated people, particularly the pilots, should be a well-trained, well-seasoned and disciplined force. It is critical to not only the Air Force, but to the United States of America." Going on to say "what we have needed to do for some time, and what is a primary focus now is the fighter force. Specifically, the F-22 will leverage the other systems that we have, and we'll follow-up with the low mix in the Joint Strike Fighter program. So, in the fighter equation, to ensure we retain a capable force, as our F-15s, F-117s, and F-16s age, I feel that our most important system for modernization is the F-22. There are some other important systems out there for the future, for example, the airborne laser and many space systems. But the F-22 is our leading edge capability, our premier leverage system that will be devastatingly first in to give us undoubted air supremacy." (See: "On Course With the New Chief." *Air Force News Agency*, December 1997, n.p. On-line. Internet, December 1997. Available from www.af.mil/news/airman/1297/csaf2.htm.)

[152] Ibid.

Notes

[153] Ibid.

[154] Ms Druyun's comments were not in regard to this research paper, although relevant. Ms Druyun also noted that "The Air Force's recent shift in focus to space operations also is reflected in the service's spending priorities Over the next five years, the Air Force will spend $23 billion on developing and fielding new satellites, space-based weapons and communications systems." (See: Cahlink, George. "Replacing an Aging Fleet." *Government Executive*, 1 August 2001. GovExec.com. On-line. Internet, 1 August 2001, n.p. Available from http://www.govexec.com/top200/01top/s7.htm.)

[155] Dr. Loren B Thompson. "US Must Reverse Bomber Blueprint, Air Force Dominated by tactical fighter community, experts say." *National Defense*, July/Aug 1999, n.p. .On-line. Internet, 2 January 2002. Available from http://www.lexingtoninstitute.org /defense/revbmb.htm.

[156] In fact, of the 4000 aircraft in the Air Force inventory, only 5% are heavy bombers.

[157] The Pentagon Panel recommendations: 1) "[I]ntegrate a series of implausibly optimistic assumptions about future bomber requirements into a report that concludes the current heavy bomber force is probably adequate to meet national needs for the next forty years; 2) [P]ropose to spend less than 1% of the Air Force's investment budget on bomber modernization, 3) [P]ropose a series of phased improvements (e.g. radars, navigation equipment, computers, etc.) Welch's Panel concluded that upgrades begin 30% sooner than suggested, 4) [A]nticipate new bomber design will begin ~2020, production to begin in 2034 and OIC in 2037. Welch's panel anticipated shortfalls would begin emerging in aircraft numbers and capabilities around 2013, probably requiring new bomber production. The bomber roadmap does not project such problems until over twenty years later and 5) Defers near-term improvements to the B-2 until 2015. Similarly, the Welch panel called for near-term enhancement of B-2 stealth features, whereas the roadmap defers most such work until 2015." (See: Thompson, "US Must Reverse Bomber Blueprint.")

[158] Col (ret) Robert Chandler argued that integrating SAC and TAC into ACC deprived the AF of "an adequate forum for planning a rapid-response, long-range bombing campaign and assessing the attendant risks." Chandler's thesis, endorsed by some members of Congress and retired general officers, is that planning for future strike requirements migrated to a community dominated by fighter pilots. This community, which has dominated Air Force leadership since the end of the Cold War, is said to favor tactical aircraft (fighter-bombers such as the F-15E) over heavy bombers for future strike missions." This thesis is likewise supported by Michael Worden's conclusions in his book Rise of the Fighter Generals and by SAAS and GO aero rating statistics. (See: Thompson, "US Must Reverse Bomber Blueprint.")

[159] Mark Selinger. "Senate Panel OK's USAF's 767 Lease Plan." Aviation Week & Space Technology, 5 Dec 01, n.p. On-line. Internet, 1 Jan 2002. Available from http://www.aviationnow.com/avnow/news/channel_military.jsp?view=story&id=news/m7671205.xml

[160] Loren B. Thompson, PhD. "The Future of Airborne Electronic Warfare." Lexington Institute. Available ON-line Internet. http://www.navyleague.org

Notes

[161] Representative Joseph R. Pitts. "Electronic-Warfare Assets Badly Neglected." *National Defense*, June 2000, 39.

[162] For example, the USN is becoming increasingly and heavily reliant on network-centric warfare as is the USCG (with its reliance on Dynamic Positioning and Steel Web) to optimize its force protection roles, as well as the Army.

[163] Subsequent to the advent of nuclear weapons, the AF became singularly focused on their promise--first as a decisive force, but then as a deterrent. When nuclear war became so implausible, adversaries re-surfaced other forms of warfare--limited warfare, terrorism, and information operations. *The US arsenal had become so powerful, it had become impotent, because that power was so one-dimensional.*[163] The same may be true today. No peer competition will emerge to <u>directly</u> challenge the US Armed Forces,[163] but they will attack, and they will attack asymmetrically. While the USAF now has a some capability against asymmetric threats, that capability is girded by information, and the USAF it has not yet developed the infrastructure to protect it.

[164] Department of Defense. *Quadrennial Defense Review Report*. Washington DC: U.S. Government Printing Office, Sep 2001,

[165] Bruce Rolfsen. "On-the-job-testing." *Air Force Times*. 21 Jan 2002, 12-13.

[166] Ibid.

[167] Ibid.

[168] QDR, 21.

[169] The Balkan air war confirmed several basic lessons about electronic warfare. First, the proliferation of advanced air-defense systems around the world has severely compromised the survivability of nonstealthy aircraft unless they receive continuous EW protection in combat.

[170] In recent Air Force tests, a B-2 with upgraded stealth was able to fly between an F-15 and F-16 operating about 20 mi. apart without being seen visually or electronically. (See: Fulghum, David A. "Stealthy UAVs Snag Rumsfeld's Attention." Aviation Week and Space Technology, 4 Jun 01.)

[171] In the case of the Air Force F-117A "stealth fighter" that was lost in combat, the F-117A was operating too far from the *Prowler* supporting it to receive effective EW coverage.

[172] In the case of the Air Force F-117A "stealth fighter" that was lost in combat, the F-117A was operating too far from the *Prowler* supporting it to receive effective EW coverage.

[173] David A Fulghum. "Stealthy UAVs Snag Rumsfeld's Attention." *Aviation Week and Space Technology* 4 Jun 01.

[174] "The overarching focus of [JV202] is full spectrum dominance--achieved through the interdependent application of dominant maneuver, precision engagement, focused logistics, and full dimensional protection. . . . The evolution of these elements over the next two decades will be strongly influenced by two factors. First, the continued development and proliferation of information technologies will substantially change the conduct of military operations." (See: U.S. Department of Defense. *Joint Vision 2020*. Washington DC: US Government Printing Office, Jun 2000, 3.)

Notes

[175] "Information technology offers U.S. forces the potential of conducting joint operations more effectively, with smaller forces and fewer weapon systems." (See: QDR, 46.)

[176] Enhanced C4ISR is necessary for SOF "to remain in contact with their commanders and to ensure access to real-time intelligence in a number of forms." (See: QDR, 46.)

[177] "Denying enemies sanctuary by providing persistent surveillance, tracking, and rapid engagement with high-volume precision strike." (See: QDR, 38.)

[178] "Kosovo underscored the need for high-capacity, interoperable communications systems that can rapidly transmit information over secure, jam-resistant datalinks to support joint forces" (See: QDR, 45.)

[179] Peter B. Teets, Undersecretary of the USAF and DNRO noted that: "The problems . . .have been a mix of unclear requirements, inadequate funding, and poor program management. He stated that he wanted " to re-emphasize the virtue and value of strong program management and that he "he will be looking at ways to apply NRO program management practices to Air Force acquisition". (See: Weinberger, Sharon. " Space Acquisition Programs Face 'Serious' Problems, Teets says." *Aviation Week & Space Technology*, 27 Feb 02. On-line. Internet, 28 February 2002. Available from http://www.aviationnow.com/avnow/news/channel_military.jsp?view=story&id=news/steet0227.xml)

[180] Unified Command Plan: For Instructional Purposes. NP Coursebook. 29 Sep 1999.

[181] Maj Shawn P. Rife, "On Space Power Separatism," 393.

[182] Paul Mann. "Air Defenses Key to Homeland Mission. *Aviation Week & Space Technology*, 6 May 2002, 26-28.

[183] Ibid.

[184]Orbital mechanics and aerodynamics are simply two different sets of laws. For example, atmospheric drag in space speeds up a spacecraft whereas drag slows down an aircraft. No pilot will decelerate his aircraft in order to accelerate.

[185] Note that the Air Force was **not** the first service to recognize the merits of space. Explorer I, the US's first satellite, was a Navy satellite. The first navigation satellites (the Transit constellation) were Navy assets as well. And the first ICBMs were developed and fielded by the US Army.

[186] The Navy's sealift assets move 99% of DoD's assets.

[187] The other services are becoming critically dependent on the Infosphere as well. The Army is likewise developing a new uniform that could transmit a soldier's location, view in multiple bands, and even indicate his/her physical status reliably. The Navy is also attempting to transform itself under the concept of Network Centric Warfare (NCW). Under NCW, several ships afloat, ashore, subsurface, in the air, and in space, work together as one coordinated team. The USN thus has become critically dependent on C4ISR and the requisite protection of its Infosphere. The Navy notes that "every facet of the Navy's continued operational primacy is in the concept of [NCW].

Notes

[188] These four decades include several major conflicts, the advent of the ICBM force, the drive toward nuclear superiority, to nuclear equivalence, to Mutual Assured Destruction, the development of stealth, and the exploitation of space.

[189] These ratios were confirmed during a lecture by a source who requested anonymity.

[190] Held prisoner on the island of Crete, Daedelus, a famous Greek engineer (and the man that designed the Minotaur's Labyrinth), fashioned two pairs of wings made of twigs, wax and feathers, for him and his son to escape the island. He cautioned his son not to fly too high as the sun's heat would melt the wax and the wings would disintegrate. Icarus failed to heed the warning.

[191] Smith, James M. "USAF Culture and Cohesion: Building and Air and Space Force for a 21st Century." Institute for National Strategic Studies. Occasional Paper 19. Colorado Springs, CO: USAF Institute for National Security Studies, June 1998, 6.

[192] Smith, "USAF Culture and Cohesion," 6.

[193] DAL was to **"**examine and recommend actions necessary to prepare the USAF Total Force for leadership into the 21st Century. It is an initiative instituted by then-CSAF Gen Meyers, after (according to MGen Link), the CSAF could not find a single general officer (GO) with the breadth and depth required to fill a critical vacancy.

[194] Unfortunately, the study was predicated on an "Air and Space Force" a term that pervaded the briefing, with IO given minimal discussion.

[195] Link, Maj Gen (ret) Chuck Developing Aerospace Leaders: Presentation to Air Command and Staff College. Maxwell AFB, AL: 17 August 2001, 12.

[196] Even today, the 13xx space career field itself is fractionated. A Missileer when asked his/her core function will note that they are missileers, not space operators. Space operators in turn, do not consider missileers true space operators.

[197] "Profile: MGen(S) Michael Hamel--Slow, Steady Path to Success." *Space News*, 21 January 2002, 22.

[198] The results were compiled from both AFPC and an independent 1997 INSS study.

[199] Vernon Loeb and Thomas E. Ricks. "l's And 0's Replacing Bullets In U.S. Arsenal." *Washington Post*. 2 February 2002, n.p.

[200] Ibid.

[201] "SAAS Homepage." Air University website. On-line. Internet, 4 January 2002, n.p. Available from http://www.maxwell.af.mil/au/saas/hist_org.htm.

[202] Interoperability is the ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces, and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Interoperability requirements are clearly stated, and seldom waived. The QDR is clear on its criticality. "Interoperability, which enables joint and combined operations, is a key element in all DoD operational and systems architectures. Experience shows that fixing systems after the fact to achieve interoperability is typically costly and often fails to satisfy mission requirements and creates security problems. The better approach is to incorporate interoperability at the outset in designing new systems." (See: Department of Defense. Quadrennial Defense Review Report. Washington DC: U.S. Government Printing Office, Sep 2001, 54 and US Department of Defense. Joint

Notes

Publication 1-02: Department of Defense Dictionary of Military and Associated Terms. Washington, DC., 12 April 2001 (as amended through 15 October 2001), 221.).

[203] QDR, 38.

[204] David A. Fulghum. "Pentagon Priorities Shift to Data and Networks." *Aviation Week and Space Technology*, 22 April 2002. For example, commercial satellite imagery contracted for **OEF** was being delivered *by hand*, requiring the imagery first be downloaded, burned onto CDs, flown to Prince Sultan Airbase, and then "hand-delivered to 15 sites within the [AOR]." (See: Jason Bates. "US Battles to Use Commercial Images." *Space News*. 8 April 2002, 1.)

[205] Weinberger, Sharon. "Intelligence, Surveillance, Reconnaissance Assets 'Woefully Short,' Says USAFE Commander." *Aerospace Daily*. 25 Jan 2002, n.p.

[206] The Department shall address and resolve critical interoperability and supportability concerns that surface during C4ISP reviews either prior to milestone or decision approval or through tasking in the Acquisition Decision Memorandum (ADM). The initial C4ISP is due at program initiation.

[207] CJCS Instruction 3170.01B requires users to develop an interoperability KPP and identify Information Exchange Requirements. The ORD sponsor shall develop IERs and associated interoperability KPP using mission-area integrated architectures as prescribed in DoD Instruction 4630.8 . . . CJCS Instruction 6212.01B. . . .the ORD sponsor shall characterize information interoperability, as applicable, within a family of systems, a mission area, and a mission, for all IT systems, including NSS.

[208] Just as the ACTS students in the interwar period poured over and synthesized data on American vulnerabilities, they soon learned that reversing the lessons learned showed adversary vulnerabilities.

[209] OSD/C3I promulgates objectives and standards to individual services, but they do not control the funding. Each of the C2 houses--CECOM, SPAWAR, and ESC have C2 integrated Program Offices (CIPOs) comprised of 20 officers in a one-third split between the department, but they have only liaison authority. They communicate, they do not control.

[210] Major capabilities to conduct IO include, but are not limited to, OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include CAN [emphasis added.] (See: US Department of Defense. Joint Publication 3-13: Joint Doctrine for Information Operations. Washington, DC., 9 Oct 1998, II-19.

[211] An evolution from the Space Battle Management Core System (SBMCS)

[212] While they are all purportedly aiming toward the Global Command and Control System (GCCS), there is significant redundancy and misallocation of sparse resources--mainly due to inter-service parochialism.

[213] Kendall, Anthony. "The Creative Leader." In *Leadership and Communication Coursebook Academic year 2002*. Compiled by Col(s) James Forsyth and LtCol Glenn Cobb. Air Command and Staff College: Department of Leadership and Communications Studies. Maxwell, AFB, AL. Aug 2001, 212.Leadership and Command Coursebook, 4.

[214] Ibid.

[215] Ibid.

Notes

[216] Acquisition Categories are designated with a "D" for DoD or "C" for component (i.e. Service)

[217] FY2000 constant dollars

[218] "AP-772: Acquisition Oversight, Review, and Decision Authority." *Acquisition Policy Course* in Advanced Program Management Course Handbook, Defense Systems Management College, Fort Belvoir, VA, May 2001, 15-61.

[219] DoD's top acquisition school for training acquisition officers from all services to better understand acquisition principles.

[220] AP class notes, May 2001.

[221] Any acquisition community in DoD is comprised of several common elements: The Government managers (officers and Government civil service), System Engineering and technical Assistance (SETA) contractors used mainly as technical support and "hands-and-feet", Federally Funded Research and Development Corporations (FFRDCs, e.g. Aerospace Corporation, RAND, Mitre, and CNA), and a contractor base.

[222] Gen Lord, AFSPC/CC, also acknowledges the biggest C2ISR challenge is "an intellectual one," i.e. people. (See: "USAF Aims to Force C2ISR Into a 'Weapon.' *Aviation Week & Space Technology,* 6 May 2002, 54.)

[223] Both have come under heavy scrutiny by the Secretary of the Air Force who is demanding wholesale restructure of several of the more significant space acquisition programs, including SBIRS, noting several key space programs have "slipped into disarray" and are facing "serious difficulties." (See: Jeremy Singer. "In Shaky Times, Pentagon Eyes Future Space Capabilities." *Space News.* 8 April 2002, 6, 46.

[224] In fact the DoD drives only 15% of the requirements in the communication industry, 5% of the requirements in the computer industry, and has no influence in the software industry. Industry has noted their deficiency and is moving smartly to remain competitive, unlike its military customer. For example, Northrop Grumman (N-G) is attempting to take-over TRW Inc. The take-over "highlights the areas U.S. weapons makers now find important -- space and information, rather than steel and firepower." N-G's strategy is based on filling its gaps in those areas, in that it has the corporate EW and stealth background (N-G builds the B-2 Spirit.) Jeff Bialos, former DUSD for industrial base issues noted "The prime [contractor] of the future is a firm that can integrate onto a platform all the defense electronics and facilitate terrific connectivity between that platform and others in a system-of-systems world." (See: "Contractors Target New Technologies -- And Each Other." *Washington Post.* 23 February 23, 2002, n.p.)

[225] Intellectual property rights are the most valued assets of leading-edge technology companies. Congressman Davis' Technology Committee was formed in part to look at options concerning the "looming crisis in the information technology (IT) and acquisition workforces, and former U.S. Department of Labor Secretary Elaine Chao, noted the crisis in government employment is "**no more evident than with the technology workforce** [emphasis in original.]"[225] This structure likewise follows Dr. Arnold Kanter's and Margiolli's recommendation as well. Dr. Kanter notes that "High technology enterprises in the non-military sector might offer relevant inputs for USAF cohesion issues," while Dr. Margiolli additionally notes "support functions, removed from the flightline and silo, exhibited a more bureaucratic orientation and closer integration with civilian specialists,

Notes

tending more toward occupational identifications . . in such an atmosphere, technology management is more prized than combat leadership." (See: US House. *HEARING NOTICE: Transforming the IT and Acquisition Workforces: Using Market-Based Pay, Recruiting and Retention Strategies to Make the Federal Government an Employer of Choice for IT and Acquisition Employees.* 101st Congress, Subcommittee on Technology and Procurement Policy, 2 Oct 01. n.p).

[226] Gregory J. Rattray. *Strategic Warfare in Cyberspace.* (The MIT Press. Cambridge, MA), 66.

[227] Note: although the US Coast Guard is also a DoD service, its wartime role, when it is transferred from the Department of Transportation to the Department of the Navy, serves the Navy's needs. Therefore, it was not included in the table.

[228] The Role of the Marine Corps in the National Defense

[229] Ibid

[230] Ibid

[231] Ibid

[232] Note: although the US Coast Guard is also a DoD service, its wartime role, when it is transferred from the Department of Transportation to the Department of the Navy, serves the Navy's needs. Therefore, it was not included in the table.

Chapter 5

Materiel Solution: The Information Service

> *The Department's leadership recognizes that continuing 'business as usual' within the Department is not a viable option given the new strategic era and the internal and external challenges facing the U.S. military. Without transformation, the U.S. military will not be prepared to meet emerging challenges.*
>
> —2001 QDR

> *This is a major change for both military and industry, and it requires thinking not in terms of platforms, but in terms of capabilities. It asks generations of program managers and defense officials to let go of traditional ways of defining themselves and recognize that end-user requirements ultimately drive any market--not just what contractors might want to sell or what acquisition officials or politicians might want to procure. It isn't easy for any institution--public or private--with a legacy of building things to begin to define itself by capabilities--not commodities. But we must.*
>
> —James Albaugh

In terms of I-Service, Chapter 2 described the threat as broad an enduring, Chapter 3 discussed the need, and Chapter 4 proved a non-materiel solution was required. Section 4 of a Mission Needs Statement[233] analyzes a *materiel* solution--i.e. it addresses current systems that could counter the threat identified earlier. That materiel solution must comply with national policy as promulgated in the NSS, QDR and JV2020. Thus the resultant solution must rectify the aforementioned concerns, namely integration and the need for a core industrial base supporting a military structure that can both fulfill its Title 10 requirements for a Service, as well as transfer its combatant forces to a combatant commander. Based on QDR goals, a potential I-Service could be constructed along four basic tenets:

a. Fulfill Title 10 Obligations. A service's function is rooted in the central purpose of the combat forces it supports--to fight the nation's wars. A service recruits, organizes, trains and equips forces which combatant commanders employ to prosecute the nation's wars. C4ISR and its defensive IO analog should be acquired under a pervasive construct by the very nature of how it is used. A *service* acquires the capabilities forces bring to war. Thus, the I-Service must also train/equip a small, elite force that is authorized[234] to "pull the trigger" when its forces are transferred to a Joint Force Commander. Government civilians and contractors[235] cannot take up offensive arms against a nation as a legal combatant. James Adams, author of the *Next World War*, explained it best: ". . . the [DoD] has to step up to the plate because they have the capability and the responsibility."[236]

b. Create A Structure Similar to US Coast Guard. The I-Service must optimize the civilian-military duality of its mission while not violating Posse Comitatus. Maintaining the intent of Posse Comitatus is essential to ensure the I-Service, given the ubiquity and pervasiveness of the InfoSphere, remains firmly under civilian control and is not used against the US populace (except in warranted cases identified by appropriate legal statute.)[237] The legal structure of the Coast Guard regarding its employment provides an appropriate precedent, one the I-Service would replicate, in that it, like the USCG, would be firmly rooted in both the civilian and military realms. The Coast Guard is specifically waived from Posse Comitatus[238] due to its multi-function roles. Both VAdm Owens and RAND strongly agree the US Government has not yet researched this critical aspect of

IO. The challenge likewise supports the QDR's call to "align, consolidate, or differentiate overlapping functions of the [OSD], the Services, and the Joint Staff," which could greatly streamline the overlapping functions of the thirteen DoD agencies involved in intelligence collection and analysis.[239]

c. Consist of Minimal Government Personnel Performing Only Inherent Government Functions. Because industry drives the IT infrastructure, the traditional structure of the DoD acquisition community must also be reformed. Support would be based on a revised industrial base calculus with both traditional and new DoD partners. The QDR, re-emphasizing the tenets of Policy Letter, 92-1 *Inherent Government Functions,* demands the DoD "focus . . . on those areas that contribute directly to warfighting. Only those functions that must be performed by DoD should be kept by DoD" unambiguously delineating those categories.[240] It simply comes down to triage--the government has only enough workers to fill these inherent government functions. The GAO agrees, and highlighted "human capitol management" as a high-risk, near-term concern.[241] Industry can do the rest, and should do the rest, as *it* is driving the Information revolution.

d. Contain a Significant Industrial Component. The traditional defense industrial base has radically changed. While broader and more diversified, it's weaker from a market perspective. Booz, Allen & Hamilton cites the culpability of acquisition reform in terms of fewer competitions, the emergence of duopolies and triopolies forcing winner-loser acquisitions, and market consolidation forcing high debt, noting "as a whole, [the DoD] industry's total value is 14% of Microsoft, 17% of Intel, [and] 50% of AOL." This posture translates into Wall Street disillusionment, more capable personnel migrating to higher payoff market sectors, and the consequent need to optimize resources.[242]

The consolidation has resulted in far fewer providers which do not heavily emphasize IT. Of the three largest competitors (Lockheed-Martin, Boeing, and Raytheon), only Raytheon has a significant IT background noting “Defense contractors also sense pressure for a change building within their own ranks . . with prime contractor status going not to the company building the airframe, but to the company supplying the integration and communications links . . . but [t]oday's reality has it the reverse.”[243]

New government structures, acquisition policies, and leadership are needed to harvest industry expertise. The QDR demands acquisition revision noting the “DoD must explore options to fully redesign the way it plans, programs, and budgets.”[244] The DoD needs to truly adopt commercial practices for IT development using end-product utility as a metric. Acquisitions would be executed under a trial system whereby the Congress would agree to freeze accounts for its top priority programs,[245] cap total costs, and freeze requirements. Information programs would then be locked, and built in blocks, harvesting the leaner acquisition approaches articulated in the revised DoDD “5000” acquisition series. Strong support from the Subcommittee on Technology and Procurement Policy would re-enfranchise the IT industry, and engenders both the QDR’s demands for necessary transformation, and Secretary Aldridge’s demand for Acquisition *Excellence* vice Acquisition *Reform*.

James F. Albaugh, President and Chief Executive Officer of Boeing Space and Communications, emphasized this industrial-military synergy at the Apr 2002 National Space Symposium, punctuating three major goals of the 2001 QDR--a **capabilities-driven** force structure, **acquisition reform** (in line with Aldridge’s vector), and **interoperability**--as well as the QDR’s pillar for “[d]eveloping transformational capabilities through increased and wide-ranging science and technology, selective increases in procurement, and innovations in DoD processes."[246] Albaugh noted:

> "While the [DoD] is transforming itself for the 21st century to achieve full spectrum dominance in order to address emerging threats, industry is undergoing a similar transformation, striving to become more competitive and adapt to a changing marketplace. The success of these efforts is **mutually dependent** now more than ever, the future of our industry lies in the **successful convergence of military and communications capabilities**. Whether we call it ubiquitous connectivity in the commercial arena, or integrated battlespace for the military one, the future of this industry--and its enormous growth potential--lies in providing a common operating picture, global situational awareness, seamless communication and information connectivity to a variety of users. . . .The key to achieving this transformational connectivity and full information superiority is development of **a single architecture that is network-centric and capabilities driven.**" [emphasis added.][247]

The traditional DoD industrial base is on-board. The IT industry can be better utilized. The QDR has provided DoD both the mandate and the vector. It is time to act.

Notes

[233] Potential Materiel Alternatives. Identify known systems or programs addressing similar needs that are deployed or are in development or production by any of the Services, agencies, or allied nations. Discuss the potential for inter-Service or allied cooperation. Indicate potential areas of study for concept exploration, including the use of existing US or allied military or commercial systems, including modified commercial systems or product improvements of existing systems." (See: CJCS 3170.01B. *Requirements Generation System*, 15 Apr 2001, C-A-1.)

[234] "[S]oldiers are trained when to use or not to use . . .force. Escalation is the rule. The military exists to carry out the external mission of defending the nation. Thus, in an encounter with a person identified with the enemy, soldiers need not be cognizant of individual rights, and the use of deadly force is authorized without any aggressive or bad act by that person."(See: "The Posse Comitatus Act: A Principle in Need of Renewal." Washington University Quarterly. (Volume 75. Summer 1997 No. 2.), 1.

[235] Except through Presidential Findings (e.g. CIA actions)

[236] "Epic cyberattack reveals cracks in U.S. defense." CNN/Sci-tech.com, 10 May 2001, n.p. On-line. Internet, 20 December 2002. Available from http://www.cnn.com/2001/tech/Internet/05/10/3.year.cyberattacck.idg/index.html.

[237] Posse Comitatus "embodies the traditional American principle of separating civilian and military authority and currently forbids the use of the Army and Air Force to enforce civilian laws." However, exceptions have been granted and are being granted on an increasing basis. The exceptions include aiding drug-trafficking (which later expanded

into the armed forces becoming "single lead agency" in drug interdiction efforts), and in domestic problems including the bombing of the Muir building, as well as in matters of intelligence with respect to the United States Coast Guard (USCG).

[238] The PCA criminalizes, effectively prohibiting, the use of the Army or the Air Force as a posse comitatus [11] to execute the laws of the United States. It reads: "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both." ."(See: "The Posse Comitatus Act: A Principle in Need of Renewal." Washington University Quarterly. (Volume 75. Summer 1997 No. 2.), 1.

[239] Today, intelligence is a vital element in every substantial international activity of the US government. The goal of intelligence is "to support decisionmakers with the best possible information, no matter its source." To perform this continuous, monumental task, the Intelligence Community, headed by the CIA and collectively known as "the 13 tribes," gathers, interprets, and analyzes intelligence while preventing allies and adversaries from doing the same. A series of statutes and Executive Orders provides legal authority for the conduct of intelligence activities. Key documents include the National Security Act of 1947 (as amended), which provides the basic organization of the US's national security effort, and Executive Order 12333, which provides current guidelines for the conduct of intelligence activities and the composition of the Intelligence Community. (See: "Unites States Intelligence Community." www. cia.gov, 15 June 1998, n.p. On-line. Internet, 30 November 2001. Available from http://www.cia.gov/ic/icagen2.htm.)

[240] These categories are: 1. "Functions directly linked to warfighting and best performed by the federal government. In these areas, DoD will invest in process and technology to improve performance." 2. "Functions indirectly linked to warfighting capability that must be shared by the public and private sectors. In these areas, DoD will seek to define new models of public-private partnerships to improve performance." 3. "Functions not linked to warfighting and best performed by the private sector. In these areas, DoD will seek to privatize or outsource entire functions or define new mechanisms for partnerships with private firms or other public agencies." (See: QDR, 61-2.)

[241] Arquilla agrees, noting: "whereas DoD once could effectively creates industry standards in order to enhance security through its leading edge role in [R&D] and its buying power, the market now set the standards"…." The National Academy of Public Administration (NAPA) developed a four-part plan to incentivize government workers. Their landmark report entitled *The Transforming Power of Information Technology: Making the Federal Government an Employer of Choice for IT Employees*, noted five key problems: 1) the government's human resources management system, 2) a "cumbersome recruiting process," 3) inadequate motivational tools, 4) poor learning opportunities, and 5) an accelerating pay gap." (See: US House. HEARING NOTICE and Arquilla, John and David Ronfeldt. *In Athena's Camp*.. RAND: Santa Monica, CA. 1997, 186.)

[242] "It's about engineering students wanting to be like Bill Gates, not John Glenn--an aerospace image problem that isn't going away. Government and industry leaders are concerned that the shortage of scientists and engineers in the U.S. aerospace and defense complex is getting worse, despite the partial collapse of Internet companies that were

consuming technical talent a year ago. According to F. Whitten Peters, a former Air Force secretary: 'The fundamental, bottom-line problem is America is not producing enough people who want to be engineers and work in the aerospace industry [noting aerospace] is an industry of great turbulence, return-on-capital is not great, stock prices are not very high, and the telecommunications community has been promising the world to people.' Boeing recently acknowledged it cannot find enough information technology professionals to handle all its projects." (See: William B. Scott, "Worries Deepen Over Dearth of Technical Talent." Aviation Week and Space Technology, 23 April 2001.)

[243] Industry has noted their deficiency and is moving smartly to remain competitive, unlike its military customer. For example, Northrop Grumman (N-G) is attempting to take-over TRW Inc. The take-over "highlights the areas U.S. weapons makers now find important -- space and information, rather than steel and firepower." N-G's strategy is based on filling its gaps in those areas, in that it has the corporate EW and stealth background (N-G builds the B-2 Spirit.) Jeff Bialos, former DUSD for industrial base issues noted "The prime [contractor] of the future is a firm that can integrate onto a platform all the defense electronics and facilitate terrific connectivity between that platform and others in a system-of-systems world." (See: David A. Fulghum. "Pentagon Priorities Shift to Data and Networks." *Aviation Week and Space Technology*, 22 April 2002 and "Contractors Target New Technologies -- And Each Other." *Washington Post.* 23 February 23, 2002, n.p.)

[244] QDR, 51.

[245] This method was used in at the Air Force Research Laboratory in 1998-2001, whereby the top priority programs funding was stabilized and not subject to the perennial funding cuts. Several smaller programs, absorbing the majority of cuts were eliminated, while critical programs, including Communication/Navigation Outage Forecasting Satellite (C/NOFS) and MightySat II.1 (*Sindri*) were finally able to concentrate resources on completing the program. It worked. *Sindri* flew the first DoD hyperspectral imager, and C/NOFs became the #1 priority program at the Space Experiment Requirements Board.

[246] QDR, 40.

[247] James F. Albaugh. "Space and the Fight Against Terrorism." *Space News*. 20 May 2002, 15.

Chapter 6

Concluding Arguments

Transformation is not a goal for tomorrow, but an endeavor that must be embraced in earnest today. The challenges the Nation faces do not loom in the distant future, but are here now.

—2001 QDR

Technology alone does not a revolution make; how military organizations adapt and shape new technology, military systems, and operational concepts matter much more. In France and the low countries in May 1940, the British and the French had technology and military systems at least comparable to those of the Germans. . . .But without the necessary organizational adaptation, the British and French were unable to withstand the German Blitzkrieg.

—Gulf War Airpower Survey

I am convinced that if the rate of change within an organization is less than the rate of change outside, the end is near.

—Jack Welch, former CEO, GE

Clausewitz defined *war* as simply a different phase in a relationship between political powers. The United States' military instrument exists *solely* to secure the endstate of *that phase*, i.e. to win wars. And the executive and legislative branches *organize* that military instrument so it can best achieve its *key* purpose: to win wars. In the early 1940s, after decades of doctrinal, parochial, and sometimes vitriolic debate, political leadership realized its military tool was no longer optimized for the future of warfare in an emerging bipolar international construct. *Strategic* in nature and *nuclear* in focus, this new kind of warfare required leadership to functionally separate the air component from its Army heritage in order to first mature, and then optimize its most violent instrument of policy. Bureaucratic *evolution* could not achieve the changes necessary given the inherent urgency, magnitude, and prevailing Army thought. A new service took root. Its separation did not obviate the need for land and sea forces; its separation augmented, optimized, and supported that need.

Today, it's a lot like the early 1940s again. The QDR recognizes the future of warfare has again changed and the unipolar construct it exists within is fractionating. Now *pervasive* in nature and *information-based* in focus, the DoD is sub-optimized against this burgeoning information threat, wielded by a complex spectrum of actors at all levels of the conflict spectrum. Information does not only support our national *security*, it undergirds our national *infrastructure.* It operates with a breadth Euclidian-based warfare was never designed to execute, just as land power doctrine was never designed to execute airpower doctrine. Information cannot win all wars alone, and like *its* parent half a century ago, does not obviate the need for other forces. It supports them, synergistically integrates them, and provides combatant forces to them, simultaneously meeting their equivalent, stringent requirements in terms of uniqueness, mission, functionality, and decisiveness.

In the 1960s, DoD leadership focused its power on deterring war, believing no nation would *directly* challenge its nuclear posture given US resources and prowess. Leadership was right. But instead of *direct* confrontation, new adversaries found alternative ways to achieve their national security objectives by continually thwarting the DoD's single, all-purpose nuclear tool it futilely wielded in a multifaceted conflict spectrum. *Today, it's a* *lot like the 1960s again*. That the US's kinetic force structure is now so overpowering and so overwhelming simply means adversaries will still have to employ asymmetric means at all levels of conflict to ensure power remains in balance. That's the nature of warfare. Dogmatic prescription to kinetic, geographic-based warfare prevents leadership from recognizing the nation's resulting vulnerability. As such, it is becoming critically and increasingly dependent on the one element it is neglecting.

In the early 1970s, the civilian leadership forced the different factions of its military tool to aggressively stake claim to core competencies after lengthy and severe budget drawdowns. The result was a military tool ill-prepared for direct confrontation for two decades and severe parochialism. *In some ways, it's a lot like the 1970s again*. The USAF has claimed Information Superiority as a USAF core competency, while simultaneously accepting responsibilities for several new and/or expanding roles. Yet its budget remains perennially fixed with respect to its sister services, with the same level of tenacity its own leadership applies to primacy on both a fighter-aircraft-dominated *decisive force* construct and a fighter-pilot dominated *leadership* construct. Airpower *is* critical. Its gravity *deserves* the attention only a single service focused on that vital capability provides. But the importance of the InfoSphere is growing, and as such the consequent span of control is *now* beyond the capability of any one service--the same legitimate argument the USAF used six decades ago against its Army parent.

So it's now 2002. It's a time when civilians can develop courses of action from *civilian-based*, *real-time* information *pushed* to them over *disparate*, *multiple*, *real-time civilian* communication links, anticipate and adjudicate enemy intentions, objectify their situation, *fuse* their assessments with those from civilian analyses and family members, and counter-attack. In doing so, the citizens on Flight 93 prevented strategic decapitation of the political Instrument of Power and subsequent collapse of its economic instrument, yet the DoD's immense and superior information architecture remains significantly un-connected, jeopardizing the "pointy end of *its* spear" that needs it most.

Bureaucratic evolution is not enough. Even as information becomes more critical, its development and exploitation continues to fracture among the services. The QDR provides the necessary focus, parameters, and vector. Information needs a single, objective lead which is not distracted by other core missions. This nation does not have the time or resources for a protracted turf battle over its most vulnerable CoG. That CoG has been surveilled, is being dissected, and has taken--and will continue to take--losses. The QDR calls for a single, effects-based definition from which it can build joint doctrine, enable an interoperable information-based architecture, re-interpret LOAC, develop a requisite force structure, recruit and train IO combatants, and finally achieve unity of action. And Title 10 says *those* are the roles of a service.

Appendix A

First Steps: Lessons Learned & Near-Term Actions

Lesson Learned

- Structuring the research around the tenets of the Mission Needs Analysis was crucial to retain objectivity and proved sufficiently flexible for use in analogous scenarios.
- The DoD must recognize that Information has become a sterling linchpin in our arsenal at the same time it's become a critical weakness with respect to all IOPs
- The DoD must recognize that the international security structure remains anarchistic in nature and as such guarantees there will be further conflict. That the US kinetic force structure is so overpowering and so overwhelming simply means that adversaries will employ asymmetric means at all levels of the conflict spectrum to ensure a balance of power is maintained
- The term Electronic Pearl Harbor is a poor metaphor. Electronic Blitzrieg is a more accurate term
- The Information threat is sufficiently broad and enduring with respect to time, international actors, the conflict spectrum, and the target. Current incorporation and logical extrapolation shows that scope to be beyond the span of control of any service, its unique needs are not and cannot be met within the current framework of any service, and that further neglect will leave the US infrastructure vulnerable
- The DoD must standardize the definition of Information Operations and the Infosphere before we can achieve unity of action. Potential definitions, based on the QDR, are postulated. Likewise, the DoD must appoint a single lead to preclude the fractionalization that occurred in space operations
- Information Operations, Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance, space operations and Electronic Warfare are symbiotic and should be treated as a single mission area
- The Information force would consist of a small cadre of military, supported largely by industry and an evolved defense industrial base
- The Information Force requires a similar structure to that of the Coast Guard to optimize the civilian-military duality of its mission while preserving Posse Comitatus

Near term actions

- Establish a joint definition of Information Operations and its associated battlespace to ground doctrine with a common analytical underpinning and joint vernacular
- Decommission the term "Command and Control Warfare"
- Begin mapping the American telecommunications and computer infrastructure to ascertain vulnerabilities
- Install a Special Operations Command intelligence officer within the Defense Intelligence Establishment to provide better cross-flow for global problems
- Emplace a single DoD C4ISR acquisition agency to manage all C4ISR programs
- Force a priori architectural analysis for all weapon systems vis-à-vis increasing the role of the Joint Requirements Oversight Council at the start, vice traditional milestone-driven procurement cycle

Appendix B

Details of Chapter 2: The Threat

The threat is broad and enduring with respect to time. JP 1-02 defines information as "Facts, data, or instructions in any medium or form [or] the meaning that a human assigns to data[248] by means of the known conventions used in their representation." Data and information are carried via an information system.[249] This type of information is appropriately termed information-in-warfare, information

> "which involves the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on integrated intelligence, surveillance, and reconnaissance (ISR) assets; information collection/dissemination activities; and its global navigation and positioning, weather, and communications capabilities."[250]

which properly used becomes intelligence:

> "The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding."[251]

The concern is centered on the DoD's dogmatic prescription to information-in-warfare, trained to believe information warfare and information-in-warfare are the same. They are not.

Information-In-Warfare: No war has ever been won without information dominance or equality. Hannibal's subjugation of Italy for 15 years, is an excellent example. "Hannibal set out from Nova Carthago in Spain. His object was clear--keep Italy for Carthage. His army numbered 90,000 foot [and] 12,000 cavalry."[252] He began his infamous march in 218 BC, soundly defeating the Roman legions although significantly outnumbered, in part due to exploiting in the Infosphere, simple and small as it was at the time, by four methods:

1) Propaganda: "Propaganda allowed him to demonstrate himself as "not as a conqueror but as a liberator."[253]

2) Knowledge of the enemy: He chose to attack on the day he could exploit the Roman General's weaknesses--impetuousness and arrogance[254]

3) Knowledge of the environment: Hannibal understood how to exploit weather, terrain, and geography[255]

4) Knowledge of Roman tactics: His superior knowledge of roman tactics ensured he could lure and trap them at the Battle of Trebia, and again in 217 BC at the Battle at Trasimene in 217 BC, and finally use their mass against them at Cannae.[256]

5) Most importantly, the effective integration of the elements delineated in 2-4.

American history is replete with examples of information dominance as well, where she had, or suffered from the lack of, information dominance. Airpower was in fact birthed due to the search for new ways to get *more* information *faster* to the rear echelons--the first airpower assets were in fact reconnaissance balloons. Decades later, the first heavier-than-air airplanes were still used predominantly in this role. As argued in Chapter 3 and Appendix C, space too, is essentially simply an information source.

More recent examples include tactics spanning WWI to the present day. On the first day of WWI, the British Navy "cut the five major submarine cables serving Germany, despite being signatories to, and having promulgated the 1884 Convention for Protection of Submarine Cables."[257] The Normandy invasion hinged on effective deception. Allied forces cracked German Enigma codes and successfully used Navaho codetalkers to hide its plans. Deception was again brilliantly used in the famous left-hook into Iraq with a diversionary amphibian assault into Kuwait and Desert's Storm's parallel warfare doctrine instantiated in Checkmate. NATO used its significant diplomatic pressure on EutelSat to cut off service to Serbian President Slobodan Milosovic who was using it for his propaganda machine. The US has also been the victim of information inferiority as well--the attack on Pearl Harbor, the failure of Desert One, and of course, 9/11.

Evolution: Information-in Warfare Integrated with Information Warfare. The US was also a victim of information operations in recent conflicts including Serbia, Somalia, and initially in Haiti. What made these last three so different however, was that a new kind of information was being used--Information Operations, not simply information-in-warfare. Information began to drive the US and the world in terms of culture, economics, and the source of power. Pundits declared "the world grew smaller," a metaphor only girdered by the information and the communication lines on which it is carried, and to a lesser, degree, the advent of faster, globally-capable transportation.

Information has likewise become critical in society as well, so critical that the concept became one of the fundamental Instruments of National Power, coincident with that of Economic, Military and Diplomatic.

The threat is broad and enduring with respect to the set of actors. Information is a critical aspect crossing every aspect of one's life, as well as to a significant portion of the industrialized world. Yet it can be exploited, denied, and attacked by a broad range of actors ranging from curious hackers, to state-sponsored actors, to actors at the nation-state level. The current infrastructure is riddled with vulnerabilities, some of which have been placed there by other computer attacks to discreetly compromise other vulnerabilities for future attacks. This concern was supported by Jack Brock, director of information management issues for the General Accounting Office (GAO). Mr. Brock told lawmakers "we have been looking at computer security for several years, and we find the same problem every time: poor access controls, poor system controls, poor management controls."[258] Likewise, Art Money, the assistant secretary for C4I systems, agreed, noting "The severity [of the hacker threat] has increased dramatically . . .Moonlight Maze brings a whole different, much more sophisticated approach…it also brings another dimension--no longer with hackers, but with the problem of a state-sponsored attack."[259]

Richard Clark, the White House's national coordinator for security, infrastructure protection, and counterterrorism, agreed acknowledging the number of trapdoors and other accesses constructed in Y2K remedial code outsourced to foreigners. Clark emphasized that the extent of outsourcing has made the US "extraordinarily vulnerable" to penetration and sabotage of critical computer systems [and that] an enemy could systematically disrupt banking, transportation, utilities, finance, government functions and defense." The following are such examples.

<u>State-Sponsored Information Warfare.</u>

<u>China.</u> China rallied forces to stage a week long *May Day* attack on US Sites from 30 Apr to 6 May in protest of the EP-3E incident that cost Japanese pilot, Wang Wei, his life after he collided with the USN spy plane. Over a hundred attacks per day were noted convincing the FBI to warn Internet users of the coming attack. Several sites were defaced, but little damage actually occurred. There is widespread speculation that the Chinese student were supported by their sovereign to initiate the attacks and search for vulnerabilities. Just as troubling, US students responded in kind. Hacker sites known as

Hackweiser, Poisonbox, and Prophet did manage to break into some Chinese sites and litter them with obscene material. Students on either side of the ocean, with or without state sponsorship have obviously taken matters of the state into their own hands.

Russia. Michael Vatis, deputy assistant director of the FBI's National Infrastructure Protection Center (NIPC), reported that his agency has strong evidence that a series of ongoing CNA incidents they've named "Moonlight Maze," are being executed by personnel at a Russian Academy of Sciences lab. The Moonlight Maze attackers employed distributed coordinated attacks,[260] a style of penetration that is particularly good at defeating existing defenses. Naval information warfare technologists dealt with these kinds of attacks several times prior to the Moonlight Maze attack, which targeted Navy computer networks. Some of the information stolen consists of "naval codes and data pertaining to missile guidance systems."[261] That Vatis could not answer Sen. Dianne Feinstein's (D-CA) questions as to the extent of the loss in an open forum supports the speculation that significant loss did occur.

Other State Actors. The QDR notes the growing number and necessity for other states to develop offensive information systems as well given America's symmetric and singular military dominance: "Similarly, states will likely develop offensive information operations and be compelled to devote resources to protecting critical information infrastructure from disruption, either physically or through cyber space."[262] In fact, Sen. Feinstein noted that "About a dozen countries have information warfare programs. They include Libya, Iraq, and Iran. Foreign intelligence services routinely break into American public and private sector computers, mapping power grids to find weak links, and leaving trap doors at virtually every U.S. military base."[263] This is resoundingly familiar to the

US Army Air Corps own analysis immediately prior to WWII, upon which the Combined Bomber Offensive was founded. For example:

> "According to the National Security Agency, foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and about methods to attack these systems."[264]

Non-State Actors

Insurgent. The Zapatista movement in Mexico offers a telling example. The Zapatista National Liberation Army (EZLN), began a violent uprising due to alleged human rights violations and a non-response by the Mexican government in Chiapas. The EZLN quickly turned to netwar, however, employing "civil-society activists associated with human-rights, indigenous-rights, and other types of nongovernmental organizations (NGOs) to 'swarm'--electronically as well as physically--from the United States, Canada, and elsewhere into Mexico City and Chiapas."[265] Their technique worked and Mexico was forced to provide concessions. Although the insurgent methods were not completely bloodless, the concessions came at a small price in human life, **a victory not only for the Zapistas, but for the tenets of Sun Tzu and Machiavelli as well.**

Curious and Pernicious Hackers. The following is included to highlight the nature of asymmetric attacks and inculcate the notion that a national, integrated effort is needed sooner than later. While the DoD cannot be responsible for policing the Internet due to resource limitations, constitutional rights and posse comitatus, it must recognize that its infrastructure is increasing and critically dependent on the electronic infrastructure and the industrial base that maintains and supplies it. The Government can work with industry and civil leaders lending its expertise and discipline while its partners identify its and their own vulnerabilities. Computer attacks are also skyrocketing at an unprecedented--

and exponential--rate. The CERT® Coordination Center (CERT/CC), a not-for-profit center of Internet security expertise noted,

> "the amount of malicious activity on the Internet is increasing at a frightening rate and shows no signs of slowing down anytime soon. 2001 marked the third consecutive year that the number of security incidents handled by [CERT] doubled compared with the previous year."[266]

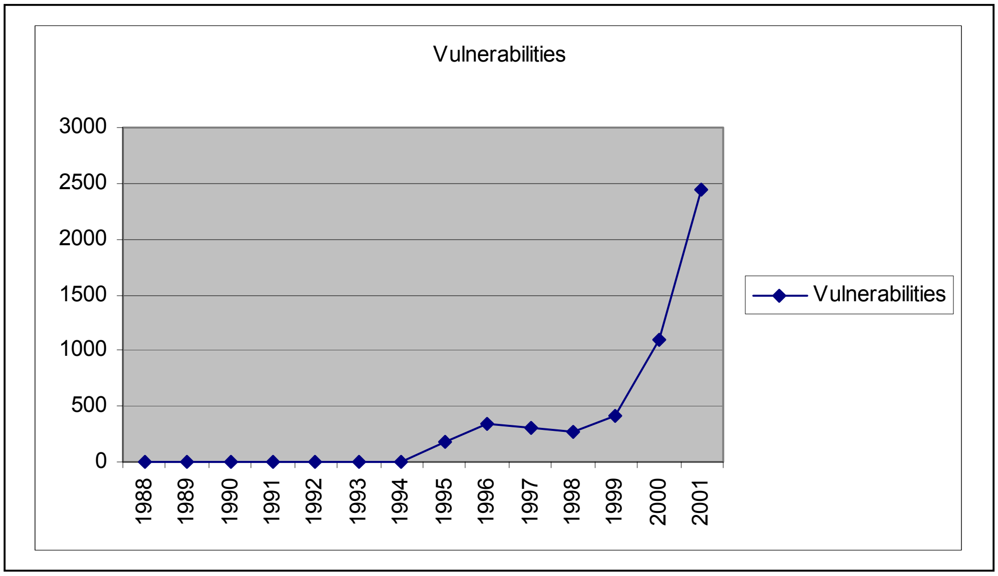


Figure 18: Increasing Vulnerabilities

Fig. 18 is included to augment the main test to show that it is not merely the increasing amount of computer usage or the increasing amount of activity on the net that artificially inflates the number of incidents, but **the number of vulnerabilities are growing as well**. This is a function of software complexity--the more complex it becomes, the more vulnerable it becomes. And these vulnerabilities exist in the same software DoD buys off the shelf, and these vulnerabilities affect DoD infrastructure as well. (Satellite planning for the MSTI-3 satellite[267] was in fact, wholly executed on an integrated suite of Microsoft Office®.

Details of some of the more significant examples follow.

Code Red & Code Red II. The Code Red Worm affected computers running Microsoft Windows NT 4.0 and Windows 2000. Like the Hollywood villain that is never dead the first time, Code Red II attacked once users were lulled into believing it had defeated its progenitor, Code Red. Code Red II, however, was more virulent, as it was self-propagating and also installed “back doors on infected computers, leaving them vulnerable to future hacking.”[268] It left the message "Hacked by the Chinese," terrifyingly familiar to the messages admitted Chinese hackers left behind after attacking DoD web severs in retaliation for the accidental bombing of the Chinese embassy. Although PRC officials fervently denied they were behind the Code Red attack, it is obvious the implications such disinformation can have on an unsuspecting public still stuck in the dogma of “primacy of print, ” one advantage the Generation-Y has over their progenitors. Code Red II impacted Qwest Communications, Microsoft, AT&T, and Federal Express. These last two are particularly disconcerting given the amount of telephone traffic handled by AT&T and Quest, the DoD’s increasing dependence on “Reachback” and the fact that due to “just-in-time” business practices, businesses as well as DoD logistics units defend heavily on FedEx. It appears as well that the US infrastructure was the primary target, accounting for almost half of the attacks world-wide, as shown in Table 16. This is not purely a function of the fact the US is “more wired” than the rest of the industrialized world--it shows the extent to which the US is dependent, and therefore the extent to which the US is vulnerable, to attack.

Nimda. Nimda is a worm that affected any computer running Windows, a particular concern to the world at large in that Windows powers 90% of the world’s computers. At a cost of only $600M, Nimda may not appear significant, even though it affected some 8.3M computer networks. But the worm did not have a destructive payload--it merely propagated and replicated email. Michael Erbschloe agreed, noting that

> “if Nimda [had had] a destructive payload it would have been a messenger sent by Satan. This would have easily cost well over three billion dollars in cleanup costs and another three billion in lost productivity if there was a killer payload and if there were no automated processes in place to eradicate the bug."[269]

Table 17: Code Red I & II Target Nations

Country	# IPs	% of Total
USA	**37318**	**42.97**
China	7818	9.00
Korea	6462	7.44
Germany	3681	4.24
Canada	3267	3.76
Great Britain	2750	3.17
Italy	1874	2.16
Australia	1821	2.10
France, Japan, Taiwan Brazil, Spain, Netherlands, Sweden, India, etc.	< 1538	< 2%

Source: Multiple

(Automated processes were developed in response to the “I Love You” virus. However, none of these automated processes, unique to each company were standardized and can be easily distributed among hacker groups to defeat them a priori.) “Nimda compromised the security of infected hosts, as it provided remote attackers with full Administrative authority over the victim and access to the entire file system.”[270] Nimda infections are further very difficult to clean, as the worm makes numerous modifications to system files and registry settings. As such, the DoD may be unable to ascertain exactly what the perpetrator gained access to, further complicating its ability to “know what the adversary knows the DoD knows.” The Nimda virus was particularly noteworthy for two reasons:

1. It acted like a coordinated system-of-systems, exploiting backdoors and security holes from previous attacks by Code Red II and others,

2. It created new security breaches, which can allow a new virus to attack

Melissa. Melissa[271] struck thousands of e-mail systems propagating across the Internet on March 26-28, 1999. “Disguised as an important message from a friend or colleague, it spread around the world like an electronic chain letter. Like Code Red, Melissa “lowered security settings on computers with Microsoft Word 97 and Microsoft Word 2000, making them vulnerable to other viruses.”[272] It acted as a precursor agent. Again, the DoD, and the world industry is wholly dependent on Microsoft® products. By sending infected email to the first 50 names in a computer user’s address book, it flooded numerous gateways forcing automatic shutdown. What is unique and more disconcerting is the nature of the message header--it was disguised as a message from an important colleague. Many of the subject lines of potential viruses are indiscreet. Discreet messages will follow as hackers better understand American culture. For example, what if the subject instead read: “Antivirus companies warn that an e-mail message asking for peace between America and Islam actually carries an extremely malicious and destructive payload.”[273] It happened and that email served as the vector to propagate Nimda in Sep 2001.

I Love You.. The "Love Letter" worm was a malicious VBScript program (the programmatic underpinning for Microsoft macros which drive keystrokes) which spread in a variety of ways. Unlike *Melissa*, the *I Love You* virus actually destroyed data. The DoD reopened public access to all of its Web sites shortly after the outbreak, only to have to close them again when Code Red II attacked. Note, however, that while public access was blocked, authorized government users had full access as well as access to the NIPRnet, which Gen Raduege, head of the Defense Information Systems Agency (DISA), calls “the command and control system for DOD, [further noting that] There is warfare out there on the Net,”[274] during an interview after the outbreak of the Code Red worms shut down access to DoD’s web. (Code Red attacked DISA’s central processing unit, filling it to 800% to 900% of its normal capacity.)

The impact of Code Red on DOD systems pales in comparison with the effect on the commercial world. Michael Zboray, chief technology officer for market researcher Gartner Group, likewise noted that “many companies' first response was to shut down email systems, paralyzing operations. In any kind of communications-intensive company, email is the de facto standard for communicating inside and outside the company.” That is a major concern for the DoD, considering it is completely dependent, moreso than any other time in history, on its industrial base. In 1996, the GAO reported that DoD’s computer systems were being attacked every day and that the DoD did not know exactly how often hackers tried to break into its computers. Defense Information Systems Agency (DISA) conducted attacks to assess vulnerabilities to find they could successfully penetrate Defense systems 65 percent of the time. While not all attacks result in actual data loss or destruction, many attacks . . .have been very serious. Hackers have stolen and destroyed sensitive data and software. They have installed “backdoors” into computer systems which allow them to surreptitiously regain entry into sensitive Defense systems. They have “crashed” entire systems and networks, denying computer service to authorized users and preventing Defense personnel from performing their duties.[275]

One of the more serious breaches occurred at Rome Laboratory, a particular concern given Rome’s work on artificial intelligence and radar guidance.

> “In March and April 1994, two British hackers attacked Rome Laboratory’s computer systems over 150 times. To make tracing their attacks

> more difficult, the hackers weaved their way through international phone switches to a computer modem in Manhattan. The two hackers used fairly common hacker techniques, including loading Trojan horses276 and sniffer277 programs, to take control of the lab's network, ultimately taking all 33 subnetworks off-line for several days. "During the attacks, the hackers stole sensitive air tasking order research data. The hackers also launched other attacks under the cover of the lab's computer systems, gaining access to systems at NASA's Goddard Space Flight Center, Wright-Patterson AFB, and Defense contractors."[278]

One hacker, "Datastream Cowboy" was caught by Scotland Yard, the second, Kuji, was never caught. **The data stolen has never been identified and no one could determine where it was sent.**

In terms of National Security, the GAO went on to report that the cost and disruption caused by these attacks is the potential threat to national security:

> Many Defense and computer systems experts believe that computer attacks are capable of disrupting communications, stealing sensitive information, and threatening our ability to execute military operations. The National Security Agency and others have acknowledged that potential adversaries are attempting to obtain such sensitive information by hacking into military computer systems. Defense officials and information systems security experts believe that over 120 foreign countries are developing information warfare techniques. These techniques allow our enemies to seize control of or harm sensitive Defense information systems or public networks which Defense relies upon for communications. Terrorists or other adversaries now have the ability to launch untraceable attacks from anywhere in the world. They could infect critical systems, including weapons and command and control systems, with sophisticated computer viruses, potentially causing them to malfunction. They could also prevent our military forces from communicating and disrupt our supply and logistics lines by attacking key Defense systems."[279]

There have been additional attacks, and the number is **doubling** every year. Some other examples include:

The U.S. Naval Academy's computer systems were attacked by hackers from several allies (Great Britain, Finland, Canada) as well as domestic universities including the University of Kansas and the University of Alabama. **The USN was unable to determine the extent of the damage and the intruder was never caught.**

Hackers attacked 34 DoD sites just prior to Desert Shield to gain information on the military strategy.

> "Using sophisticated search engines, they browsed directories and modified systems to obtain full privileges allowing them future access . . . ran automated searches for key words such as nuclear, weapons, missile, Desert Shield, and Desert Storm. They copied military data on systems at major U.S. universities, whose infrastructure was not up to par with those at the DoD sites not hacked into. [Of more concern is that] after the attacks, the hackers modified systems logs to avoid detection and to remove traces of their activities."[280]

The hackers were never caught, and the amount/extent of information stolen never ascertained.

Using the Internet as a vector, a hacker from Argentina hacked into computers at the Naval Research Laboratory, other Defense installations, NASA, and Los Alamos National Laboratory, stealing "sensitive research data". . .[on] aircraft design, radar technology, and satellite engineering, that is ultimately used in weapons and command and control systems, and reliability test data of sophisticated weaponry."[281] **Neither the Navy nor the Army were able to determine the extent of the damage or what was stolen**.

Although these are isolated cases, the GAO reported "Defense officials say they reflect the thousands of attacks experienced every year. Defense officials agreed the cost of these incidents is significant and probably totals tens or even hundreds of millions of dollars per year."[282] Again, not understanding what data was stolen, leaves the US open to even more information attacks, and compromises its war planning systems, satellite command control, and national infrastructure. The 2001 update to the 1996 report, went on to report:

> “The risks associated with our nation’s reliance on interconnected computer systems are substantial and varied. Attacks can come from anywhere in the world, over the Internet, other networks, and dial-up lines. By launching attacks across a span of communications systems and computers, attackers can effectively disguise their identity, location, and intent, thereby making them difficult and time-consuming to trace.”[283]

The threat is broad and enduring with respect to IOPS. The United States infrastructure is indeed under attack, but because the only casualties have been data, dollars, and confidence in electronic commerce, the Government has not yet fully engaged the threat. This is dogma--leadership sees war only when casualties come home. Tom Ridge, the director of Office of Homeland Security (OHS),

> “hammered home the fact that information technology now pervades everyday life--from communications and emergency services to water and electricity delivery. "Destroy the networks and you shut down America as we know it and as we live it and as we experience it every day."[284]

Former Senator Sam Nunn agrees. "There are some who believe we are going to have an electronic Pearl Harbor, so to speak, before we really make (computer security) the kind of priority that many of us believe it deserves to be."[285] Marv Langston, former deputy CIO for the Department of Defense (DoD), shares those same convictions and used the same analogy, telling news publications that the United States needs to prepare itself for an electronic Pearl Harbor. Michael Erbschloe, vice president of research at Computer Economics[286] and author of *Information Warfare: How to Survive Cyber Attacks*, agreed with the characterization and considers cyber terrorism to be an extreme threat to e-commerce and Internet applications in government, education, and business. The concern is attracting high level attention in the Government (supporting Mahan’s 6th edict of National Power--See Chapter 4), but the Government has not yet embraced this different kind of vulnerability.

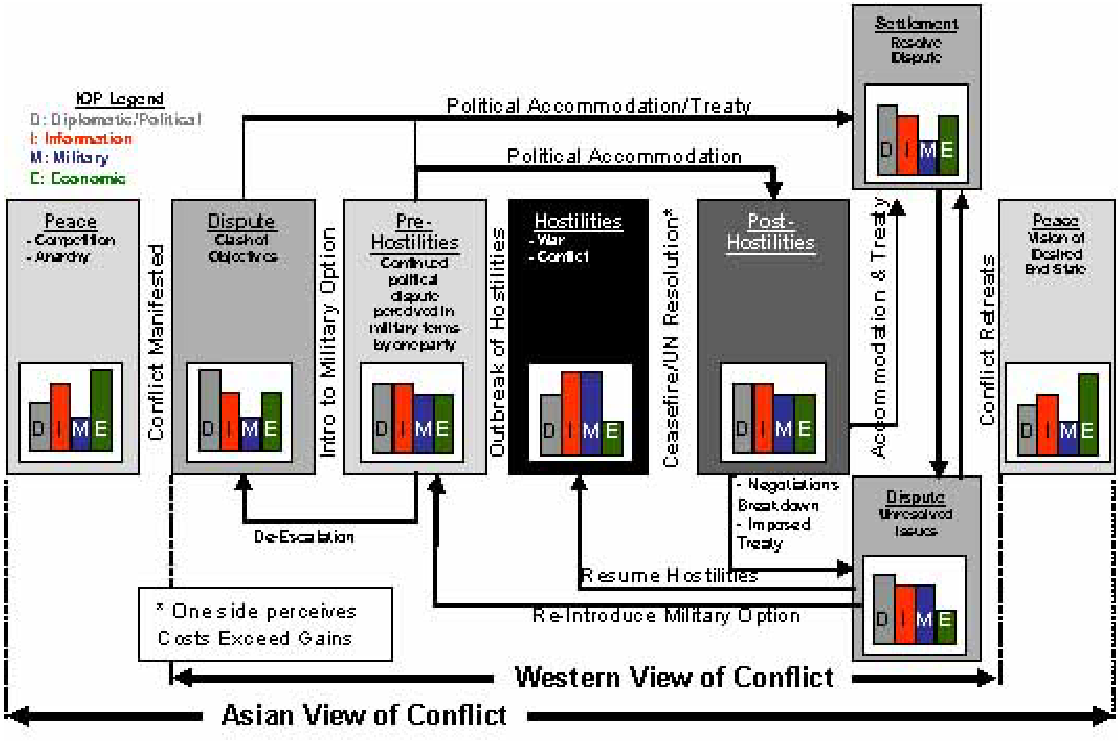


Figure 19: IOPS in the Conflict Spectrum[287]

Fig. 19 is the venerable spectrum of conflict diagram used at ACSC since 1996 to graphically summarize the contribution of each IOP throughout the many phases of conflict and in particular to the inculcate the importance of determining the end state before engaging in war. It's been updated to include the Information IOP, a term which came into vogue only in 1998 in conjunction with the publication of PDD 63. Information is critical in each of these stages, and is significantly more important given the Asian View of Conflict which believes sovereigns to be continually in conflict in all matters of state, whether outwardly manifested, or not. Table 17 explains the relative ranking of Information in each of the conflict stages, and with respect to each of the other IOPs.

Table 18: Relative Contribution of Information IOP to Other IOPS Throughout Conflict Spectrum

Conflict Stage/ Information's contribution to IOP	Diplomatic	Economic	Military
Peace	- **More important** than D-IOP because it fuels action at the international, internal, and individual level,[288] the latter being just as critical in a democracy - Fuels diplomatic efforts at the interstate level in terms of information gathering, transactions, treaty monitoring. communications and negotiations - Supports the internal information architecture ensuring national focus and prosperity - Monitors budget outlays - Informs world of US position & legitimacy	- **Less important** then E-IOP in that the US power base ATT is a result of its economy which fuels its military, internal progress, and international programs and prestige - Underpins the economic infrastructures at the international and internal levels - Trillions transferred daily by electronic means - Instantaneous market visibility - Is the circulatory system that drives the economic body	- **More important** than M-IOP because it is working in the background where the military cannot tread ATT - Provides persistent intelligence - Continually updates threat analyses used in acquisition decisions - Refines J-2 estimates for use assigning tasks in Joint Capability Strategic Capabilities Planning (JSCP) in deliberate planning - Critical to C4ISR - Critical to training - Monitors DoD budget outlays
Dispute	**- Less important** than D-IOP because the latter is at the forefront to avert conflict - Fuels diplomatic efforts at the interstate level in terms of information gathering, transactions, treaty monitoring. communications and negotiations - Used to anticipate adversary - Informs world of US position & legitimacy	- **Is as critical** to economy ATT - Underpins the economic infrastructures at the international and internal levels - Trillions transferred daily by electronic means - Instantaneous market visibility into effects dispute may have on international markets - Provides insight into enemy investment strategy	- **More important** than M-IOP because it is working in the background where the military cannot tread ATT - Provides persistent intelligence - Refines J-2 estimates for refining previous deliberate planning - Critical to C4ISR - Critical to training - Monitors budget outlays - Provides targeting options

Table 17 (Cont.): Relative Contribution of Information IOP to Other IOPS Throughout Conflict Spectrum

Conflict Stage/ Information's contribution to IOP	**Diplomatic**	**Economic**	**Military**
Pre-Hostilities	- **As important** as D-IOP as it surfaces adversary intentions, secondary goals, and underpins Flexible Deterrent Options (FDOs) - Fuels diplomatic efforts at the interstate level in terms of information gathering, transactions, treaty monitoring. Communications and negotiations - Used to anticipate adversary - Provides Flexible Deterrent Options to ensure other parties remain neutral and/or do not aid enemy - Informs world of US position & legitimacy - Provides insight into possible adversary secondary goals which may force early resolution	- **More important** than E-IOP in relation to its effect on D-IOP and M-IOP - Underpins the economic infrastructures at the international and internal levels - Trillions transferred daily by electronic means - Instantaneous market visibility into effects dispute may have on international markets	- **More important** than M-IOP as it prepares the battlespace for EW, IW, and kinetic warfare (KW) - Provides persistent intelligence - Refines J-2 estimates for Crisis Action Planning - Critical to C4ISR - Critical to training - Critical to Intelligence Preparation of the Battlefield an - Critical to pre-positioning logistics
Hostilities	- **More important** than D-IOP in relation to its criticality to M-IOP and relative decrease in D-IOP ATT - Fuels diplomatic efforts at the interstate level, communications and negotiations - Used to anticipate adversary - Provides Flexible Deterrent Options to ensure other parties remain neutral and/or do not aid enemy - Informs world of US position & legitimacy - Provides civilian leadership insight into progress of the war	- **More important** than E-IOP in relation to its criticality to M-IOP and relative decrease in E-IOP ATT - Underpins the economic infrastructures at the international and internal levels - Provides insight into enemy resources - Provides for cutting off access to funds/freezing assets - Instantaneous market visibility into effects conflict having on international markets	- **As important** to the M-IOP given criticality of C4ISR, and denying adversary C4ISR in terms of EW, IW, and KW - Provides persistent intelligence - Reduces fog and friction - Provides friendly OODA loop - Provides means to maneuver within enemy OODA loop - Critical to logistics

Table 17 (Cont.): Relative Contribution of Information IOP to Other IOPS Throughout Conflict Spectrum

Conflict Stage/ Information's contribution to IOP	**Diplomatic**	**Economic**	**Military**
Post-Hostilities	- **As important** as D-IOP - Provides best hope to ensure conflict ends in settlement vice dispute as it gives leadership the upperhand in negotiations - Fuels diplomatic efforts at the interstate level in terms of information gathering, transactions, treaty monitoring. communications and negotiations - Used to anticipate adversary actions - Informs world of US position & legitimacy - Provides insight into possible adversary secondary goals which may force early resolution - Provides best hope to ensure conflict ends in settlement vice dispute	- **More important** than E-IOP in relation to its effect on D-IOP and M-IOP - Underpins the economic infrastructures at the international and internal levels - Instantaneous market visibility into effects dispute may have on international markets	- **More important** than M-IOP as it prepares the battlespace for renewed EW, IW, and kinetic warfare (KW) and direct military actions restricted through cease-fire/treaty - Provides persistent intelligence - Refines J-2 estimates for Crisis Action Planning - Critical to C4ISR - Critical to Intelligence Preparation of the Battlefield an
Settlement	**- Less important** than D-IOP because the latter is at the forefront to avert conflict - Fuels diplomatic efforts at the interstate level in terms of information gathering, transactions, treaty monitoring. communications and negotiations - Used to anticipate adversary actions - Informs world of US position & legitimacy - Provides insight into possible adversary secondary goals which may force early resolution	- **As important** as E-IOP as the latter regains its position of primacy in transition to peace - Underpins the economic infrastructures at the international and internal levels - Supports nation-building	- **More important** than M-IOP as it prepares the battlespace for EW, IW, and kinetic warfare (KW) in Dispute - Provides persistent intelligence - Refines J-2 estimates for Crisis Action Planning - Critical to Intelligence Preparation of the Battlefield - Critical to redeployment

Table 17 (Cont.): Relative Contribution of Information IOP to Other IOPS Throughout Conflict Spectrum

Conflict Stage/ Information's contribution to IOP	**Diplomatic**	**Economic**	**Military**
Dispute	**- Less important** than D-IOP because the latter is at the forefront to avert conflict - Fuels diplomatic efforts at the interstate level in terms of information gathering, transactions, treaty monitoring. communications and negotiations - Used to anticipate adversary actions - Informs world of US position & legitimacy - Provides insight into possible adversary secondary goals which may force early resolution	- **More important** than E-IOP in relation to its effect on D-IOP and M-IOP - Underpins the economic infrastructures at the international and internal levels - Supports nation-building	- **As important** to the M-IOP given criticality of C4ISR, and ability to deny adversary C4ISR in terms of EW, IW, and KW - Provides persistent intelligence - Refines J-2 estimates for Crisis Action Planning - Critical to Intelligence Preparation of the Battlefield - Critical to redeployment

Company CEOs and national and state public policy officials convened a conference hosted by former U.S. Sen. Sam Nunn to discuss the need for cooperation between the corporate, academic, government, and civil worlds on fighting computer attacks. Senator Nunn noted that "Experts point out that U.S. infrastructure, such as water supply, telecommunications, transportation and financial systems, will increasingly be accessible --and managed--with the help of the Internet. And that could make them vulnerable to cyber-age attacks."[289]

Y2K: One source of great infrastructure concern is the sheer amount of Y2K fixes that were outsourced to foreign countries for economic reasons as well as for reasons of immediacy--by American industry, including the DoD. Foreigners could have easily installed backdoors which can be penetrated at later time--a sort of electronic mole. This is not the "super-secret" espionage it appears to be. In 1997, Intel® was widely criticized when it was revealed it had written code into its processors that could identify the user and their search patterns for subsequent consumer targeting. Terril D. Maynard, a CIA analyst attached to the NIPC emphasized that: "The use of untested foreign sources for Y2K remediation has created a unique opportunity for foreign countries or companies to access and disrupt sensitive national security and proprietary information systems."[290]

In light of this growing concern, President Clinton issued PDD 63 "The Clinton Administration's Policy on Critical Infrastructure Protection" in May 1998 to inculcate "a cooperative public-private approach to protecting the nation's critical infrastructures." PDD 63 was based on the President's Commission on Critical Infrastructure Protection, an independent panel comprised of leading civil, military and industrial leaders to ascertain the extent the US was reliant on the Information Infrastructure and vulnerable to adversary Information Operations.[291] Figure 20 displays these eight critical infrastructure elements. Orange elements are critically dependent on the information infrastructure, purple ones are significantly dependent, and the grey one is somewhat dependent. Vulnerabilities are portrayed by the line extending from the center of the information hub--lines completely bisecting the element indicate extreme vulnerability. **The panel concluded the US was in no immediate danger, but that the danger was real, was growing, and the US was growing more vulnerable:**

> "…we found all our infrastructures **increasingly dependent** on information and communications systems that criss-cross the nation and span the globe. That dependence is the source of **rising vulnerabilities** and, therefore, it is where we concentrated our effort. We found no evidence of an impending cyber attack which could have a debilitating effect on the nation's critical infrastructures. While we see no electronic disaster around the corner, this is no basis for complacency. We did find widespread capability to exploit infrastructure vulnerabilities. **The capability to do harm—particularly through information networks--is real; it is grow-**

ing at an alarming rate; and we have little defense against it [emphasis added.]"[292]

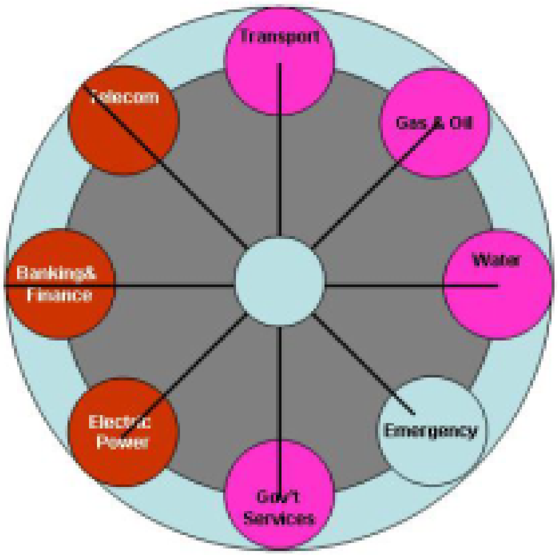


Figure 20: Eight Critical US Infrastructures

Nor is there [adequate] data on infrastructure vulnerabilities. This lack of preparation can be contrasted with the APWD work, where ACTS, originally concerned with US vice European vulnerabilities, discovered by reversing the problem, they could instead ascertain German targets. PDD 63 delineated eight infrastructure segments (Fig. 20) and assigned various Government agencies assigned to determine their vulnerabilities. Unfortunately, two critical foci are missing: 1) cross-flow between the segments with the possible exception of telecommunications and banking, and 2) strategic analysis. In terms of cross-flow, for example, while the Department of Transportation investigated the transportation industry--there is no evidence it was likewise looking at the shipping and CRAF'ing required to ship troops and supplies. The Department of Energy may be considering the overall vulnerability of the power grids, but is the military then considering its dependence on that power grid?

Telecommunications is a particular concern. The Air Force Institute of technology (AFIT) sponsored Capt Jeffrey Del Vecchio in researching the vulnerability of DoD phone networks in that many DoD phone calls travel trough international switches mainly to optimize economics. He noted:

> "Both government and industry **have viable concerns whether or not their messages are both secure from an adversary** as well as to the reliability of the message reaching its destination. …**Today's PSTN's may have security and reliability risk due to the path a message may be sent** . . .[s]ince many government agencies use Public Switched Telephone Networks (PSTN) for official voice messages. . . "[emphasis added.][293]

His research found critical dependencies and security concerns making DoD links, including secure DSN links, highly susceptible to tampering, re-routing, and monitoring by any adversary--military, or economic. The more significant concern is that the DoD is unaware of the vulnerability of its systems--again thinking in Euclidean terms. The caller imagines the line being connected directly from his office to the other party's handset, unaware of the fact that call can be carried over multiple lines, multiplexed, sent over SatCom, fiber, copper, or submarine cable, and may even pass through foreign gateways. He arguably concluded that for a small Government investment, the civilian telecommunications industry could greatly increase information assurance. Industry won't make the investment in that it is a matter of economics. The Government must. He noted:

> "It is neither the lack of technical expertise nor patriotism that causes a [Network Service Provider (NSP)] to be a member of a coalition that has a network that may be vulnerable to adversary tampering. Instead, it is the lack of finances and possible incentive to form a stronger coalition and upgrade their network's invulnerability. Networks are primarily designed by the industry to withstand *statistical* failure. **A planned attack by an adversary may not be taken into account when a NSP designs a network or forms a coalition**. . . .In the highly competitive industry of voice communication, large amounts of investments are needed to keep up with ever changing industry standards. These investments are naturally invested in areas of concern that return the most revenue.[294] Vulnerability as a whole returns little or no contributions to the NSP's revenue [and]

> **any system designed purely for financial efficiency under normal operating conditions is highly susceptible to intentional disruption** [emphasis added.]"[295]

However, most analyses of attacks have focused on the tactical, verse strategic goals of attackers. Tactical support investigates attacks as singular incidents of identified vulnerabilities. "Examples of tactical support include analysis of (1) a computer virus delivery mechanism to issue immediate guidance on ways to prevent or mitigate damage related to an imminent threat or (2) a specific computer intrusion or set of intrusions to determine the perpetrator, motive, and method of attack."[296] Strategic analysis looks at trends and analyzes singular threats as part of a broader whole, for example, as an attack against a national vulnerability. "Strategic analyses are intended to provide policymakers with information that they can use to anticipate and prepare for attacks, thereby diminishing [potential damage.]"[297] Since its establishment, has focused its resources on the tactical. The GAO reports that strategic analyses has been lacking in that

> ". . . no generally accepted methodology for strategic analysis of cyber threats to the nation's infrastructures has been developed. Lacking are a standard terminology [(See Chapter 3)], a standard set of factors to consider, and established thresholds for determining the sophistication of attack techniques."[298]

The report cited the lack of staff in general, and experienced staff in particular. This is true not just in the DoD, but throughout the Government. The FBI in particular "lacks staff who are experienced in critical infrastructure operations and intelligence analysis."[299] GAO assessed progress on PDD 63's objectives goals five years after PDD 63 and noted that industry had completed few of their assessments and none of the five committees had reported all required analyses to the NIPC. The objective simply lacks an executive agent. PDD 63 is on the right track, but its follow-through is being managed by those that simply do not understand operational art--in particular, centers of gravity, timing and tempo, and decisive points.

The threat is broad and enduring with respect to the spectrum of conflict.

One of the more objective reasons space has not matured to the point that it can become its own separate service is the reality that offensive space-based weapons have not been developed. Until space has a true force application capability, it does not meet the criteria of a service to organize, train, and equip true offensive forces. As noted in Chapter 3, offensive weapons will likely take the form of ground-based or even space-based jammers, but all EW is IO. IO, however, has been used by non-state actors, by US Armed Forces, and by adversaries against the United States. Example follow:

Operation Enduring Freedom. The US exercised its diplomatic instrument of power to strike a blow at Somalia's government, economy, and civilian infrastructure when it convinced AT&T and British Telecom, "Somalia's only internet company and a key telecommunications network" to cut off its international gateway. The Internet is particularly critical to Somalia, a country that has an adhoc feudal based government and no banking or telecommunications infrastructure. The US requested the gateway be cut based on its suspicion that two firms, Somalia Internet Company and al-Barakaat, are terrorist links supporting Al Qaeda. "The closures have severely restricted international telephone lines and shut down vitally needed money transfer facilities. Correspondents say the closure of the companies will have a devastating effect on the country, which desperately needs the services they provide, in that 80% of Somalis depend on money they receive from relatives outside the country. There is significant collateral damage as well, in that “the United Nations, local and international aid agencies, as well as the government itself all relied heavily on internet access, now denied.”[300]

Peacekeeping: Humanitarian Efforts. Operation Restore Democracy. Haiti was the first example where a set of phased information operations were developed and not fully executed given the success of the first IO phase. The first phase consisted of classic psyops, exploiting the EM spectrum, and exploiting the media. Planners for Restore Democracy ordered “Voice of America to step up the frequency of Creole broadcasts to Haiti, make more frequencies available for broadcasts that supported the American invasion” and deliver pocket radios to the Haitians by airdrops. Compass Call, using its two 10kW transmitters than blasted pro-American and pro-Aristide propaganda. CNN was tipped off of the fearsome deployment of troops to show the junta what they were facing. Many wisely chose not to engage. Phase I succeeded. Phase II consisted of weapons to shut down the water and electricity, immobilize gas pumps to prevent junta refueling, and jammers to spoof [local radio and television stations to insert pro-Aristide programs.” Classic Psyops and the media precluded use as junta resistance collapsed.[301]

Peace Enforcement: Operation Deliberate Force. Gen. Henry Shelton, chairman of the Joint Chiefs of Staff, revealed that the United States did indeed wage information warfare as part of the NATO bombing campaign. While the DoD did not penetrate banking networks, as wildly reported, IW did target Yugoslavia’s Integrated Air Defense System network. However, “[c]oncerns about international legal constraints on electronic information warfare . . .deterred American government hackers from exercising their full capabilities. Moreover, the Pentagon says it is hampered by a lack of a national information operations vision and strategy.” . . .The conduct of integrated information operations was hampered by the lack of advance planning and necessary strategic guidance to define key objectives."[302]

Major Theater War: Desert Storm. The Gulf War was the first Information war--a notion not just captured by American or coalition partners, but by Soviet and Chinese forces as well. The United States unveiled a radically new form of warfare in the Persian Gulf in 1991. By leveraging information, US and allied forces brought to warfare a degree of flexibility, synchronization, speed and precision heretofore unknown. By exploiting knowledge, it devastated Iraq's formidable military machine"--and showed the world what to expect, and how to prepare. It exposed US dependence, and therefore US vulnerabilities. "Because of the strategies of deception, maneuver and speed employed by coalition forces in DESERT STORM, knowledge came to rival weapons and tactics in importance, giving credence to the notion that an enemy might be brought to its knees principally through destruction and disruption of the means for command and control." Information dominance has always been a critical factor in war, as described in the first part of this chapter. But Col Campden correctly notes that "DESERT STORM was different . .. it was a war where an ounce of silicon in a computer may have had more effect than a ton of depleted uranium . . ." Yet, despite the brilliant Checkmate campaign, it was only the arrangement of the targets and the inclusion of the leadership as a target that differentiated the Desert Storm air campaign from other campaigns. The Gulf War Survey concluded that "With few exceptions, the planners of Desert Storm used the same target categories as in previous wars. In World War II, Korea, and Vietnam, aircraft attacked air defenses, fielded armies, oil refineries, electrical power grids, and, even command, control, and communications." The difference was the parallel effect achieved through information--" . . . the dependence of modem military organizations on vast amounts of information, and the relative ease with which communications technology could disseminate that information."[303] As noted by LtGen S. Bogdanov, Chief of the General Staff Center for Operational and Strategic Studies (FSU): "Iraq lost the war before it even began. This was a war of intelligence, EW, command and control, and counterintelligence. Iraqi troops were blinded and deafened. Modern war can be won by informatika and that is now vital for both the US and USSR."[304]

Notes

[248] Data: "the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. (See Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms,* 12 April 2001 (as amended through 15 October 2001), 117.

[249] Information System: The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information (See Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms* (as amended through 15 October 2001), 209.

[250] Air Force Doctrine Document 2-5.2 Intelligence, Surveillance and reconnaissance Operations, 21 Apr 1999.

[251] Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms* (as amended through 15 October 2001), 209.

[252] "Cannae Toolbook Text." In Air Command and Staff College Distance Learning Program. Lesson TH504r02. CD-ROM ACSC Multimedia Edited Version 2.2., Aug 1997, n.p.

[253] Ibid.

[254] Hannibal knew Flaminus, the Roman commander. "True to form, Flaminus advanced early the next morning with no reconnaissance, no advance or flank guards. A heavy, mist-like fog hung over the area and screened the hills from view. Surprise was complete and the battle was really decided before a blow was struck." His exploitation of Infosphere at Cannae resulted in the textbook application of the double envelopment and the massacre of 70,00 Roman troops. Hannibal's efficient intelligence system soon informed him that Varro was the more impetuous of his opponents, and so Hannibal decided to force an action on a day Varro was in overall command. "At Cannae (Barletta, Italy, today), the Romans were determined to crush Hannibal's center." As Hannibal's men were forced back, they found themselves slowly backing up a slope. The top of the slope formed a "V" if viewed from above, and the [Hannibal's] Spaniards and Celts now formed a concave line that conformed to that "V," with [his] African squares still anchored to their original positions at the tips. Due to the nature of the terrain, the Romans fought uphill as they advanced and at the same time were restricted into a narrowing front

as their mass of men entered the "V." Although the Roman infantrymen did not know it, their fate was all but sealed by this time. Hannibal had planned for his cavalry to strike the decisive blows while his infantry fought a large-scale delaying action. By that time, the Roman infantry had fought its way up the slope and into the closed end of the "V," the point. As the men became more tightly packed into a confined space, fewer of them could use their weapons effectively." And when, finally, it was over, the Roman army had been truly annihilated. Of the original force of 86,400, "some 71,500 Romans were dead or captured—83 percent of the entire army. Carthaginian losses were less than 6,000." (See: "Cannae Toolbook Text." In Air Command and Staff College Distance Learning Program. Lesson TH504r02. CD-ROM ACSC Multimedia Edited Version 2.2., Aug 1997, n.p.)

[255] Hannibal knew the weather and the terrain, turning that information into a Course of Action whereby he could pin whole Roman legions by attacking through the Apennines and Arnus swamps, and trapping them against Lake Tresimene.

[256] Hannibal was fully versed in the tactics of the Roman legions. "Two new consuls, Caius Terentius Varro and Aemilius Paulus, were given command of the combined legions of Rome with orders to make an end to the feared Carthaginian. Normally, the two consuls would have independent commands but, by custom, when their forces were combined, command of the whole alternated daily.

[257] Department of Defense Office of General Counsel. *An Assessment of International Legal Issues in Information Operations,* May 1999. On-line. Internet, 10 January 2002. Available http://www.terrorism.com/documents/dod-io-legal.pdf.&

[258] Kimery. Anthony. "Moonlight Maze." *MIT-KMI.com,* 3 Dec 99, n.p. On-line. Internet, 20 December 2001. Available from http://www.mit-kmi.com/3_6_art1.htm.

[259] Ibid.

[260] Distributed coordinated attacks use hundreds or thousands of servers to attack a single server. Because so many servers are used, each attack can be camouflaged as a legitimate connection attempt, making it difficult for the victim's intrusion software to know that it is under attack, and impossible to identify just who is attacking.

[261] Anthony Kimery. "Moonlight Maze." *MIT-KMI.com,* 3 Dec 99, n.p. On-line. Internet, 20 December 2001. Available from http://www.mit-kmi.com/3_6_art1.htm.

[262] US Department of Defense. *Quadrennial Defense Review Report*. Washington DC: U.S. Government Printing Office, Sep 2001, 15.

[263] Kimery, "Moonlight Maze."

[264] General Accounting Office. *"Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities"*, April 2001. GAO-01-323, April 2001, 8.

[265] Arquilla, John and David Ronfeldt. *Networks and Netwars*. (RAND: Santa Monica, CA. 2001), 178.

[266] This is a frightening analogy to Moore's law which predicts that processing speed doubles every 18 months. Yet this indicates even a faster rate--12 months vice 18 months.

[267] The third experiment in the Miniature Sensor Technology Integration series (MSTI-3) is a small Air Force Research Laboratory satellite developed for BMDO and

carries SWIR, MWIR, and visible cameras to gather characteristic background data for the Air Force.

[268] Elinor Mills Abreu. "Damage from Code Red worms continuing to add up." *Infoworld.com*, 8 August 2001, n.p. On-line. Internet, 20 December 2001. Available from http://iwsun4.infoworld.com/articles/hn/xml/01/08/08/010808hnredcosts.xml.

[269] "Analyst estimates Internet virus hit eight million systems." *ABC News Online*, 3 October 2001, n.p. On-line. Internet, 20 December 2001. Available from http://www.abc.net.au/news/science/computers/2001/10/item20011003022605_1.htm.

[270] "CERT® Advisory CA-2001-26 Nimda Worm." *CERT.org,* 25 Sep 2001, n.p. On-line. Internet,. 20 December 2001. Available from http://www.cert.org/advisories/CA-2001-26.html.

[271] "W97M.Melissa.A (also known as W97M.Mailissa) is a typical macro virus which has an unusual payload. When a user opens an infected document, the virus will attempt to e-mail a copy of this document to up to 50 other people, using Microsoft Outlook." (See: Raul K. Elnitiarta. "W97.Melissa.A." *Symantec Security Update,* 29 March 1999, n.p. On-line. Internet, 26 December 2001. Available from www.symantec.com/avcenter/venc/data/mailissa.html.

[272] Raul K. Elnitiarta. "W97.Melissa.A." Symantec Security Update, 29 March 1999, n.p. On-line. Internet, 26 December 2001. Available from www.symantec.com/avcenter/venc/data/mailissa.html.

[273] "Worms continue Internet attacks." CNET.com, 25 Sep 2001. On-line. Internet, 26 December 2001, n.p. Available from http://news.com.com/2009-1001-273186.html?legacy=cnet.

[274] Paul Festa and Joe Wilcox. "Experts estimate damages in the billions for bug." *CNET.com*, 5 May 2000, n.p. On-line. Internet, 20 December 2001. Available from http://news.cnet.com/news/0-1003-200-1814907.html.

[275] General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Report GAO/T-AIMD-96-92*, 22 May 96, 7.

[276] Trojan horses are programs that when called by authorized users perform useful functions, but that also perform unauthorized functions, often usurping the privileges of the user. They may also add "backdoors" into a system which hackers can exploit.

[277] Sniffer programs surreptitiously collect information passing through networks, including user identifications and passwords.

[278] Air tasking orders are the messages military commanders send during wartime to pilots; the orders provide information on air battle tactics, such as where the enemy is located and what targets are to be attacked.

[279] General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Testimony of Jack Brock. Report GAO/T-AIMD-96-92*, 22 May 96, 7.

[280] General Accounting Office. "Defense Information Security." *www.pbs.org*, May 1996, n.p. On-line. Internet, 20 December 2001. Available from http://www.pbs.org/wgbh/pages/frontline/shows/hackers/risks/dodattacks.html.

[281] GAO, *Computer Attacks at Department of Defense Pose Increasing Risks*, 7.

[282] Ibid, 28.

Notes

[283] Ibid, 22.

[284] Michael J. Miller. "The Cyberterrorism Threat." *pcmag.com*, 27 Nov 2001, n.p. On-line. Internet, 21 December 2001. Available from . Available at http://www.pcmag.com/article/0,2997,s%253D1499%2526a%253D17512,00.asp.

[285] "Heading Off an 'Electronic Pearl Harbor': CEOs, policy leaders discuss cyber-security at forum." *CNN.com*, 6 April 1998, n.p. On-line. Internet, 24 December 2001. Available from http://www.cnn.com/TECH/computing/9804/06/computer.security/.

[286] *Computer Economics* analyzes the economic impact of malicious code attacks.

[287] Note: The original chart from 95-053 was used as a baseline, and modified for the Information IOP and the changing calculus of the international environment. (See: "ACSC Research Project 95-053: Planning and Execution of Conflict Termination." In Air Command and Staff College Distance Learning Program. Lesson Wc503r05. CD-ROM ACSC Multimedia Edited Version 2.2., Aug 1997, n.p.)

[288] Interestingly enough, being critical to the three images identified by Waltz.

[289] "Heading Off an 'Electronic Pearl Harbor': CEOs, policy leaders discuss cyber-security at forum." *CNN.com*, 6 April 1998, n.p. On-line. Internet, 24 December 2001. Available from http://www.cnn.com/TECH/computing/9804/06/computer.security/.

[290] Anthony Kimery. "Moonlight Maze." *MIT-KMI.com,* 3 Dec 99, n.p. On-line. Internet, 20 December 2001. Available from http://www.mit-kmi.com/3_6_art1.htm.

[291] The panel, created under Executive Order 13010 designated as "*critical* certain infrastructures whose incapacity or destruction would have a debilitating impact on our defense or economic security. Eight were named: telecommunications; electrical power; gas and oil storage and transportation; banking and finance; transportation; water supply; emergency services (including emergency medical services, police, fire and rescue); and government services." (See: President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* Office of the President. Washington DC: US Government Printing Office, October 1997, A-1.)

[292] President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* Office of the President. Washington DC: US Government Printing Office, October 1997, i.

[293] "Currently, the Department of Defense (DoD) relies on the Public Switched Telephone Networks (PSTN) for the bulk of its telecommunications. The PSTN is a composite of multiple interconnected networks, where each network is operated, maintained, and managed independently from the others. …However, the network operators … rely a great deal on each other for routing calls to destinations outside of their network span. Based on worked out agreements among the service providers, they decide on how and where they will physically interconnect their networks. These physical points of interconnection are called Points of Presence (POPs). In today's world of the telecommunications, there is much concern with the reliability and security of a given network. (See: Capt Jeffrey R. Del Vecchio, "An Incentive Model for Secure International Telecommunications." Thesis. Presented to Department of Systems and Engineering Management Graduate School of Engineering and Management Air Force Institute of Technology. Air University. Air Education and Training Command. March 2000, 22).

Notes

[294] "Commercial telecommunications companies have been involved with vulnerability of their networks since the civil war when military messages where sent via telegraph, sometimes directly to the President himself. During World War II, Bell Telephone employees reestablished telecommunications in Germany and France so that military commanders would have a reliable system to transmit messages. AT&T, during the cold war, routed much of their telephone lines around major cities to prevent the physical damage that may be caused by an adversary's nuclear strike. Today, the physical damage is not as important as it was in the past. We must now worry about the "intentional translation of a single digit in a million lines of computer code, which, without instant remedy, can easily deny service to much of the national telecommunication system." (See: Del Vecchio, Jeffrey R. "An Incentive Model for Secure International Telecommunications." Thesis. Presented to Department of Systems and Engineering Management Graduate School of Engineering and Management Air Force Institute of Technology. Air University. Air Education and Training Command. March 2000, 22).

[295] Capt Jeffrey R. Del Vecchio. "An Incentive Model for Secure International Telecommunications." Thesis. Presented to Department of Systems and Engineering Management Graduate School of Engineering and Management Air Force Institute of Technology. Air University. Air Education and Training Command. March 2000, 22

[296] General Accounting Office. *"Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities"*, April 2001. GAO-01-323, April 2001, 39.

[297] GAO, *Critical Infrastructure Protection*, 39.

[298] Ibid.

[299] Ibid, 42.

[300] US Shuts Down Somalia Internet." British Broadcasting Company, n.p. On-line. Internet, 23 November 2001. Available from http://news.bbc.co.uk/hi/english/world/africa/newsid_1672000.stm.

[301] See: Adams, James. *The Next World War*. New York: Simon and Shuster. 1998, 97.

[302] US Department of Defense. *Report to Congress. Kosovo/Allied Force After Action Report.* Washington D.C.: U.S. Government Printing Office, 31 Jan 2000, 98.

[303] Thomas A. Keaney and Eliot A. Cohen. *Gulf War Air Power Survey Summary Report*. Department of Defense. Washington D.C., 1993, 248.

[304] US Department of Defense. Joint Publication 3-13. *Joint Doctrine for Information Operations*. Washington, DC., 9 Oct 1998, II-15.

Appendix C

Details of Chapter 3: The Need

Definitional Conflict

Politics is Power. Power is the ability to compel one to act in a desired way. The body politic uses a number of political means to achieve its objectives, i.e. it's desire way. The literal translation of 'politik' has three components: politics (international efforts), policy (internal efforts), and history (how the nation acts based on its value structure). Thus each of the political means (war, diplomacy, etc.) must support each of these three components. As such, each element comprising that means, must likewise comply with these three components, as depicted in Fig. 21.

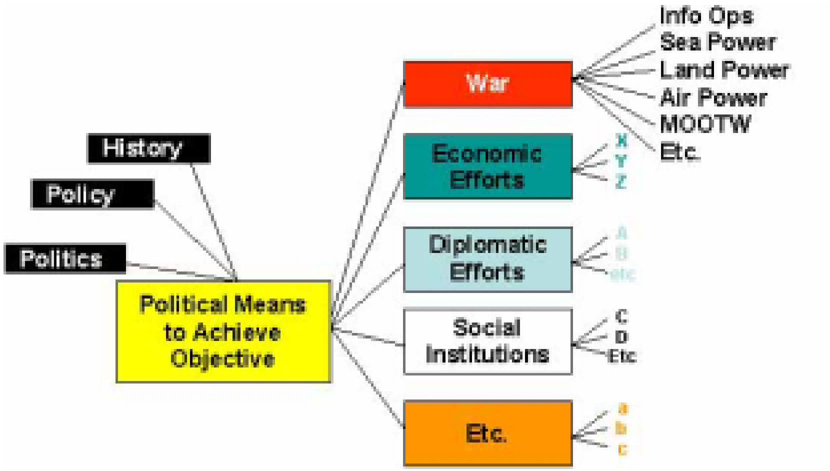


Figure 21: Every Instrument of War Must Fully Support Politik

The Joint Staff is likewise finding it difficult to determine the nature of IO. In a J-7 briefing given to ACSC, Col Gildner noted IO was one of the most immature definitions in trying to characterize the conflict spectrum, as shown in Fig. 22.

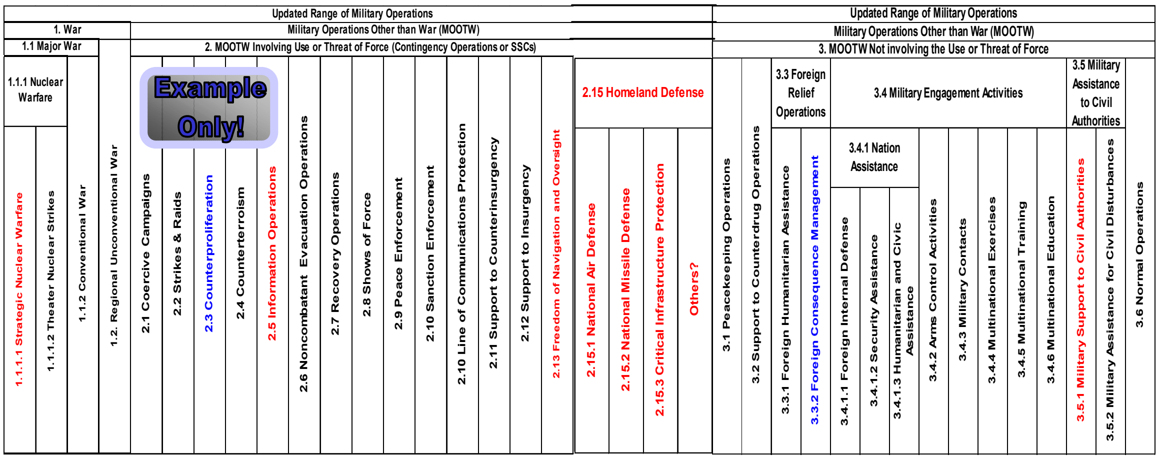

Updated Range of Military Operations
1. War
Military Operations Other than War (MOOTW)
1.1 Major War
2. MOOTW Involving Use or Threat of Force (Contingency Operations or SSCs)
1.1.1 Nuclear Warfare
1.1.1.1 Strategic Nuclear Warfare
1.1.1.2 Theater Nuclear Strikes
1.1.2 Conventional War
1.2. Regional Unconventional War
2.1 Coercive Campaigns
2.2 Strikes & Raids
2.3 Counterproliferation
2.4 Counterterroism
2.5 Information Operations
2.6 Noncombatant Evacuation Operations
2.7 Recovery Operations
2.8 Shows of Force
2.9 Peace Enforcement
2.10 Sanction Enforcement
2.10 Line of Communications Protection
2.11 Support to Counterinsurgency
2.12 Support to Insurgency
2.13 Freedom of Navigation and Oversight
2.15 Homeland Defense
2.15.1 National Air Defense
2.15.2 National Missile Defense
2.15.3 Critical Infrastructure Protection
Others?
Updated Range of Military Operations
Military Operations Other than War (MOOTW)
3. MOOTW Not involving the Use or Threat of Force
3.1 Peacekeeping Operations
3.2 Support to Counterdrug Operations
3.3 Foreign Relief Operations
3.3.1 Foreign Humanitarian Assistance
3.3.2 Foreign Consequence Management
3.4 Military Engagement Activities
3.4.1 Nation Assistance
3.4.1.1 Foreign Internal Defense
3.4.1.2 Security Assistance
3.4.1.3 Humanitarian and Civic Assistance
3.4.2 Arms Control Activities
3.4.3 Military Contacts
3.4.4 Multinational Exercises
3.4.5 Multinational Training
3.4.6 Multinational Education
3.5 Military Assistance to Civil Authorities
3.5.1 Military Support to Civil Authorities
3.5.2 Military Assistance for Civil Disturbances
3.6 Normal Operations

Figure 22: Information Operations Remains Undefined at Joint Level[305]

Why Other Umbrella Concepts Are Deficient

C4ISR

The Air Force, recognizing this inherent synergy, birthed the terms Command, Control, Communications, and Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR). However, it has an inherently passive underpinning--it does not in itself carry out offensive operations.

Information Superiority

Information Superiority, which has conflicted definitions among the services, is foremost a degree of Information Dominance.

Netwar and Cyberwar

Netwar is defined as “an emerging form of conflict (and crime) at societal levels, short of traditional military warfare, in which protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age."[306] Many different definitions exist for cyber warfare but all have the same tone--cyber warfare attacks software and is an act of war. As such, the other critical elements are not included, peacetime and defensive use is not applicable, and in fact, cyber warfare does not even address its necessary transport vector. Neither Joint nor Service Publications define Cyberwarfare. According to USAF LtCol Lionel Alford, cyberwarfare is

> "Any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system [and] includes the following modes of cyber attack: cyber infiltration, cyber manipulation, cyber assault, and cyber raid."[307]

Command and Control Warfare (C2W)

For the same reasons, computer network attack and computer network defense simply target one element of the C4ISR construct. Thus the DoD developed the concept of "command and control warfare," techniques that encompass OPSEC, deception, psychological operations, electronic warfare, and physical destruction. The concern with the definition is that it is only applicable in wartime, and does not begin to handle the defensive aspect of information operations. In addition, C2W is completely centered on its target: command and control, vice the true effectiveness--the manipulation of data, information, or intelligence. What of computer attack and denial of communications? The concept is akin to developing *bunker* warfare, or *airfield* warfare, or *artillery* warfare--the concept is too narrow and obscures the true target: the mind of the enemy commander, his strategy. The objective of war is to bend the enemy to your will, not to pulverize his forces. C2W does not embrace this. Capen and Dearth likewise agree the C2W term should be retired, noting its antiquity and the illogical groupings of its elements.[308]

Electronic Warfare

Joint Publication 1-02 defines electronic warfare as

> "any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy, [further defining electronic attack as] a subset of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires."[309]

Congressman Pitts agrees as well that EW is at least a form, if not a subset of Information Operations. Pitts writes:

> "For a variety of bureaucratic and doctrinal reasons, the armed services today prefer to differentiate electronic and information warfare. But from a purely practical perspective, it is obvious that EW has always been about controlling the electromagnetic spectrum in wartime so that we can know the enemy better than he knows us." He goes on say that "low observables (stealth) are just one in a series of measures conceived to preserve electromagnetic dominance."[310]

Figure 23: Physical Tracers have Analogs in the EM Environment

Thus integrating the fields of space control and information operations is crucial in this regard. The space community could synthesize decades of man-hours of lessons learned studying how the air-breathing and land forces have employed EW.

A common warning in employing tracer bullets (See Fig. 23) is that tracers are always "two-way"--they indicate the position of the attacker as well as that of the target. This is the principle behind the High-speed Antiradiation Missile (HARM)--when an adversary radar sweeps its AOR for hostile aircraft, sophisticated electronics packages on the HARM lock on the radar beam and once fixed, can hit the target even after the radar is turned off. EW is largely the same way--a Prowler brute-force jamming a radar site can easily be tracked and would be a somewhat suicidal mission if US strike packages were not so overwhelming. If the US did not have the advantage of lethality, the Prowler would be easily tracked--again, EW tracers work the same way. Likewise space control jammers would have to employ covert jamming techniques or use the fire and move techniques common to ground artillery, in that they would have to be in the footprint of the satellite they are jamming, which may be within hostile territory.

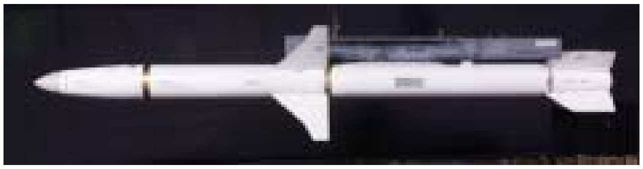


Figure 24: High-Seed Anti-Radiation Missile

But electronic warfare is not the umbrella concept either because it is only applicable in the electromagnetic spectrum. Communications traverse many different mediums, and those mediums will only proliferate and differentiate. Fiber optics is a good example, and their use is growing in the commercial industry which has supported its 4000% growth over the p decade.[311] As fiber optics become more prevalent new ways will have to be devised to protect and/or attack the information they carry. This may not employ EW techniques. Exquisite intel can reveal those links, which may or may not exist in the EW spectrum. Fiber optics are particularly important in this context based on future development. Developing nations lack the current Public Switched Telephone Network (PSTN) structure existing in first-world countries. Third-world countries as they progress will therefore wire the country with high-bandwidth delivery systems--fiber and satellite links vice the copper that traverses the highways of first-world countries. Attacking the commander's primary PSTN node does little if he has multiple redundant back-ups. The JFC could employ maneuver warfare--place the adversary where he wants him to be by limiting his options--to force him to employ other information means. But again, it would be an attack on information, preventing the adversary from using his transmission node. Thus, EW fails to provide an applicable umbrella concept.

Space

The Air Force has thus failed to recognize however, that space is simply an information medium, its overall importance, and the joint community's definitions are still split out as if they are not one in the same. This became all too apparent in Desert Storm as well as Deliberate Force. In the latter, James Adams in "The Next World War," acknowledges this synergy, noting: "[t]he lesson that had to be learned from the Gulf War for General Franks was not how to gather more information--patently there were systems in use that were producing mountains of information--but what use was made of it once it had been acquired. The key to that was processing and transmission [emphasis added.]"[312] The same was true in Bosnia, eight years later--"A similar problem exists in Bosnia where the Predator UAV (Unmanned Aerial Vehicle) gathers vast amounts of data on points of potential conflict that have to be analyzed by large numbers of people."[313]

But the rapid emergence and even faster acceleration of the information age have left the DoD with a set of tools and an infrastructure with glaring gaps, and significant redundancies which can only force thinking along long-held paradigms. Humans need tangibles to see and touch. Satellites alone are only as useful as the data they can record and transmit. Because the NRO systems were, and largely remain behind the "green door," they are considered differently from other satellites--and worse, from different intelligence assets. They are not. They also simply carry information and it's the accuracy and precision of that information that is critical--not the asset itself. "Killing the messenger," interdicting enemy scouts, using snipers to shoot a communication line, cutting power to the ground station receiving the satellite downlink or jamming a satellite uplink outright are all facets of the same thing: denying the adversary communication and information.

All satellite payloads execute their mission, and all satellite operations are conducted through the EM spectrum. This applies to stored, near-real-time or real-time data transmission. Photo-reconnaissance satellites map imagery through electro-optics, weather satellites use active and/or passive radiometers to measure spectral characteristics, signal intelligence assets sweep EM emissions, and communication data is encoded through manipulation of radio frequency waves. In terms of the communication, this is fairly straightforward--data is digitized, transmitted to receivers, decrypted if required, decoded, and then converted into digital or analog information with no human intervention required. Payload data may then have to be analyzed through computer, mechanical and/or human intervention to be translated. It's all data, and it all resides in the EM spectrum.

Space Operations include space support (launching, retrieving, and conducting satellite operations), force enhancement (the payload the satellite executes, e.g. navigation, communication, ISR, etc.), force application (ground-ground ICBMs only) and space control. Note: No DoD satellite has ever been recovered, and few commercial and civil satellites have benefited from on-orbit maintenance.) With the notable exception of launch operations, the whole of space operations-- payload execution, and telemetry, tracking and command (TT&C) operations to downlink the payload data, is completely dependent on proper control and manipulation of the electromagnetic spectrum. In addition, it can be argued that launch operations are simply an implied task to conduct information operations, no different than "launching" a SOF team for HUMINT. This concept is supported by the routine nature of launch operations. Launch support have in fact become so routine, most have been turned over to contractors executing Total System Performance Responsibility (TSPR).

Fall CORONA 2001 made enormous strides in recognizing the difference between the air and space mediums, in noting that the term "Aerospace" a terms coined in the early 90's to show the two mediums as indistinguishable, will gradually be replaced with the term "Air and Space." Yet it refused to accept the instantiation of either a Joint Forces Space Component Commander or Joint Forces Information Component Commander. In addition, former CSAF General (ret) Michael Ryan agrees the time for a separate space force is far away, noting "there is no need for a Space Force or Corps separate from the USAF until mankind moves beyond the earth's orbit - likely at least 50 years away. . . . But it will come." The recently completed Space Commission report said a separate space entity was likely to be needed in the future, although it gave no timeline.[314]

Note as well that space systems do not support the central tenets of airpower as do air-breathing systems, as shown in Table 18.

Table 19: Space Power Conflicts with AF Core Tenets

Tenets/Principles of War	Space
Balance	None
Uniquely can be persistent	No--revisit times, easily denied through camouflage, concealment and deception (CCD)
Flexible and versatile	**Flexible: Yes & No**: **Yes**--An imager can switch its GSD, and can reroute comm pretty easily if people coordinate **No**--Very difficult to re-position, very very difficult to re-task/re-orient, tied to distinct launch ports and TT&C nodes, cannot turn an imager into a comm bird, etc. **Versatile:** Yes--supports strategic (DI, SIOP, OI, NTM), operational (comm into theater, IPB), and tactical (real-time comm and ISR, GPS, BDA)--all on the same satellite
Synergistic	Yes--critical enabler to 5 services
Prioritized	No--too many lead agencies and data, especially ISR, does not get to the people that need it most; security is overarching priority and unnecessarily restrictive
Execution decentralized/Centralized control	No--13 tribes, DISA, civil, commercial, SPACEAF (controls buses, some payloads), Army Space (control DSCS III payload), Navy Space (controls FLTSAT and its own crypto), CIA, NSA; space does TT&C, very little C2 (except for missiles)
Concentration of purpose	No--See above exacerbated by difficulty to retask

Table 20: Space In Terms Of Principles of War

Principles of Warfare	
Surprise	No--orbitology very simple to figure out and CCD easy
Unity of Command	No--13 tribes, DISA, civil, commercial, SPACEAF (controls buses, some payloads), Army Space (control DSCS III payload), Navy Space (controls FLTSAT and its own crypto), CIA, NSA
Mass	Yes--saturate ITO GPS, comm, NTM No: ISR is very limited and perennially a High-Demand-Low-Density assets
Maneuver	No--very difficult to re-position, very very difficult to re-task/re-orient, tied to distinct launch ports and trajectories and TT&C nodes (Boeing SeaLaunch helping launch flexibility); on the plus side, it is difficult to get close enough with a kinetic ASAT to be effective
Offensive	No: Definite strategic role but no ability to deliver force, decisive or otherwise
Objective	Yes--space executes its payloads well
Security	No-overly constrained resulting in stovepipes; Space assets are very vulnerable (e.g. Leonids, space Wx); some links easily jammed, others protected but very low BW. Launch prep time obvious and significant and cannot be protected due to proximity to sea; C2 nodes very vulnerable (need to augment them with redundant, protected space nodes), spoofing and MIJI (natural and man-made)
Economy of Force	Yes and No--NTM, R&D very expensive, launch very expensive ($20K/lb); significant losses; Many of the NTMs can be duplicated & improved through aircraft - HUMINT is still superior
Simplicity	No--very difficult to maneuver, re-task, TT&C simple but requires massive infrastructure, lots of personnel attrition; significant overhead in coordinating with civil, commercial, foreign suppliers

Table 21: Space Operations is a Subset of IO

Type of Source	Source	Details
Joint Doctrine	JP 3-33	Key military functions of space: "intelligence, surveillance, and reconnaissance; ballistic missile detection and early warning, weapons guidance, position location, communications, and environmental monitoring. **Space is truly the fourth medium** or military operations and represents to our terrestrial warfighters the ultimate high ground."[315]
Service Doctrine	AFDD 2-2	"The Air Force is unique in its ability to capitalize on the contributions of space systems by being able to integrate and respond with rapid mobility and firepower **to the near-real-time information afforded by systems operating in space.**"[316]
Service Doctrine	AFDD 2-2	"Adversaries may have imaging and other space systems capable of monitoring operations and the ability to adversely affect US systems. American military leaders cannot afford to have enemy commanders monitor friendly force activities, locate critical command nodes, identify maneuver elements as they deploy for combat, or witness the debarkation of forces and supplies. This **information** would substantially facilitate an adversary's war planning and execution, which could result in casualties for friendly forces."[317]
Service Doctrine	AFDD 2-2	"Space systems provide an instantaneous presence not available from terrestrial-based forces, **permitting the United States to leverage information** to influence, deter, or compel an adversary or affect a situation. The use of multiple space platforms allows warfighters to exploit the various sensors, resulting in a synergistic battlespace perspective that reduces the fog of war."[318]
Service Doctrine	AFDD 2-2	"**Although space systems provide global coverage, some can be focused to provide information on specific areas of interest**, which can improve situational awareness and planning tempo and can **enable information dominance** for all friendly military forces."[319]
Service Doctrine	AFDD 2-2	The national security space program **collects information** critical to America's national security.[320]
Service Doctrine	AFDD 2-2	"Space surveillance (broad area coverage) **provides information** vital to the reconnaissance (close scrutiny) of an area or objects of specific interest. Space surveillance identifies alterations in the space environment, such as changes in the order of battle and deployment or retirement of space systems. **Information derived from both surveillance and reconnaissance data** allows planners to identify where force application or space control is required." [321]
Service Doctrine	AFDD 2-2	"Space systems provide flexibility in meeting requirements for timely, accurate, and reliable s**pace-derived information, data products, and services**." [322]
Service Doctrine	AFDD 2-2	"Properly positioned in sufficient numbers, space-based systems could provide a global capability for much of the i**nformation** currently provided by airborne platforms such as the joint surveillance, target attack radar system (JSTARS) and the Airborne Warning and Control System (AWACS)." [323]

Table 20 (Cont.) : Space In Terms Of Principles of War

Type of Source	Source	Details
Service Doctrine	AFDD 2-2	“Offensive counterspace operations destroy or neutralize an adversary’s space systems **or the information they provide** at a time and place of our choosing through attacks on the space, terrestrial, or link elements of space systems.” [324]
Policy	QDR	“In recognition of the high-technology force multipliers provided by space systems, the QDR places increased emphasis on developing the capabilities to conduct space operations.”[325]
Legal	DoD Office of the General Council	“These systems perform such functions as communications relay, imagery collection, missile warning, navigation, weather forecasting, and signals intelligence. **In fact, it can be said that at the current stage of space activity, the exclusive functions of both military and civilian satellites are to gather and relay information**.”[326]
Leadership	USCINCSPACE	Former Secretary of the Air Force, Sheila Windall: Our space-based systems are the glue that holds our joint team together, that provides the information dominance and the global awareness that we have come to take for granted. . . . Our space-based forces are not peripheral, they're not just a frill. **They're pumping the blood of information through the body of our combat forces**.[327]
Leadership	USCINCSPACE	General Howell M. Estes II, former USCINCSPACE noted as well that “oil was the driving force of yesterday’s industrial age. What’s going to **drive the information age society? Space**.”[328]
Leadership	USAF/CC	“By continued development of space systems we gain not only **access to collect information** from denied or difficult to reach regions, we will also be **better able to communicate and command operations** in those areas. [329] “This combination of manned, unmanned and space platforms will talk together at the digital level to resolve ambiguities of target location and target identification. Together, they will provide the right information to predict the enemy’s intentions and successfully execute air operations to defend national interests.” [330] “Space and surveillance assets from all the services worked together to produce target **information** for all US aircraft. [SOF] teams on the ground helped spot targets and avoid collateral damage.”[331]
Leadership	SECAF	"We simply must find ways to get more out of our space assets -- through horizontal integration of systems, best practices and smarter management of the information we obtain from space systems."[332].

As explained above, space assets are merely information gathers and conduits, operating in a consistent EM environment. But what of space control? The QDR likewise calls for significant efforts in terms of space control. This too has been promulgated by Air Force doctrine and leadership. AFDD 2-2 states:

> "Gaining air and space superiority is a primary goal of a military campaign and must be achieved early to ensure freedom of action. Like air superiority, space superiority helps to provide the freedom to conduct operations without interference from an adversary. Hostile powers must not be permitted to freely use space systems against US national interests. The US cannot permit an adversary access to precision navigation signals, instantaneous communications between leadership and subordinate echelons, situational awareness, accurate weather data, or a host of other services that are, or will be, available from space. In future conflicts the US may have to fight for space superiority."[333]

The USAF achieves space superiority through space control:

> "Space control is the means by which space superiority is gained and maintained to assure friendly forces can use the space environment while denying its use to the enemy. *Counterspace is the mission carried out to achieve space control* objectives by gaining and maintaining control of activities conducted in or through the space environment. Offensive counterspace operations destroy or neutralize an adversary's space systems or the information they provide at a time and place of our choosing through attacks on the space, terrestrial, or link elements of space systems. Offensive counterspace operations use lethal or nonlethal means to achieve five major purposes: *deception, disruption, denial, degradation, and destruction of space assets or capabilitie*s."[334]

Table 22: The Spectrum of Realistic Space Control

Space Control Objective	**Definition**	**Permanence**	**Effect**	**Primary Means**
Deny	Elimination of the utility of the space systems, usually without physical damage.	*Temporary*	*Partial/Total*	EW
Disrupt	Impairment of the utility of space systems, usually without physical damage to the space segments. These operations include delaying critical mission data support to an adversary	*Temporary*	*Partial/Total*	EW
Degrade	Impairment of the utility of space systems usually with physical damage.	*Permanent*	*Partial*	EW
Destroy	Elimination of the utility of space systems, usually with physical damage.	*Permanent*	*Total*	EW Kinetic
Deceive	Measures designed to mislead the adversary by manipulation, distortion, or falsification of evidence	*Temporary*	*Partial/Total*	EW
Protect	Preventing adversary effects against our space systems and can be active or passive	*Permanent/ Temporary*	*Partial/Total*	Hardening Redundancy
Surveil	Long-term observations of adversary spacecraft and capabilities	*Permanent*	*Partial/Total*	EW

There are few kinetic anti-satellite (ASAT) weapons. ASATs were researched but no nation has an active kinetic kill weapon. Ground-based RF weapons are considered in the 2020 timeframe. Space-based weapons are likewise being considered, most notably the Space-Based Laser, but this too is simply manipulation and amplification of the EM spectrum. Thus space control comes down to the manipulation and exploitation of the electromagnetic spectrum--electronic warfare, practiced since 1850 after adversaries noted Morse code could be interrupted by severing land lines--or better yet--compromised without the adversary knowing.

Kinetic weapons would likely be confined to Low Earth Orbit (LEO) where many of our ISR assets reside in polar and sun-synchronous orbits. These orbital regimes are heavily populated and include only a small inclination bandwidth to optimize their orbital characteristics. They would also cause a significant debris-tracking problem for the Space Shuttle and International Space Station missions. Kinetically attacking a satellite in geosynchronous orbit would be extremely difficult given the boost capability required. However, if the weapon could obtain orbital altitude, rendezvous, and destroy the target, it would pollute the orbital regime in the highest demand, which is already overcrowded, has already caused interference problems, and is limited to a very small band in both inclination and altitude, again to exploit the advantages of geosynchronous and geostationary orbits. The Air Force was chastised by the world community for its *Celestial Eagle* Program, an F-15 based ASAT weapon that added 257 pieces of orbital debris when it destroyed Satellite P78-1, as was the USSR for its significant history in kinetic space weapons.[335]

Our space assets are indeed vulnerable. An example is the Global Positioning System (GPS). The GPS navigation system is particularly vulnerable to jamming its weak signal strength, and because it resides in the L-band of the EM spectrum. The Honorable Mr. Teets, currently the Deputy Undersecretary of the USAF for Space, in fact is strongly considering delaying the GPS III acquisition in favor channeling the funds to upgrading GPS IIF signal strength. Aviaconversia, a Russian electronics firm, showed off a portable 4-watt GPS jammer selling for $4000 at the Moscow Air Show in Sep 98.[336] Although not demonstrated, it apparently caught the eye of many people--its cost over the Internet tripled within days of the Air Show. Claims the device could blank out GPS over a 200-km radius do seem excessive, but a smaller radius is possible. Even a radius of 1 km could send PGMs off course into civilian and other non-legal targets, offering a propaganda coup for our adversaries. This capability is possible, with a simple 1KW jammer, as analytically demonstrated by RAND.

Lawrence Young, a physicist at the Jet Propulsion Laboratory in Pasadena, is confident in Russian claims, noting an engineer could build such a device, and more powerful ones, from widely available electronics.[337] USAF leadership also acknowledges the vulnerability of GPS. BGen James Armor, former director of the GPS Joint Program Office in El Segundo, California, noted that "Jamming GPS might be a useful military technique for those who might oppose US and allied forces."[338] Gen Estes strongly recommended the AF "improve the jamming resistance of GPS as soon as possible," and noted that he was "shocked that we didn't get jammed in Afghanistan."[339]

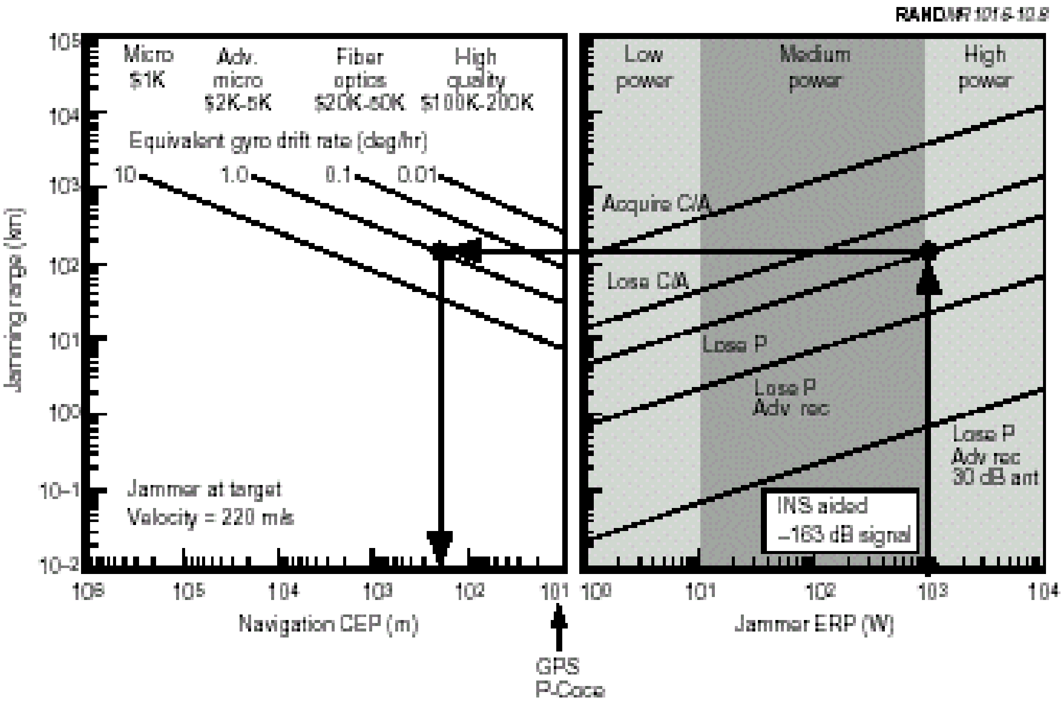


Figure 25: The Reality of GPS Jamming--Very Real, Very Simple, Very Possible[340]

Notes

[305] Col Will Gildner. "JV2020." Lecture. Dept of International Security and Military Studies. Air Command and Staff College. Maxwell AFB, AL, 9 January 2002, 25.

[306] John Arquilla and David Ronfeldt. *Networks and Netwars*. RAND: Santa Monica, CA. 2001, 6.

[307] Lionel D Alford, Jr. "Cyber Warfare: A New Doctrine and Taxonomy." On-line. Internet, 12 February 2002, n.p. Available from www.stsc.hill.af.mil/crosstalk/2001/apr/alford.asp.

[308] Alan D Campen, and Douglas H. Dearth. *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*. (AFCEA International Press. Fairfax VA, Oct 200), 102.

[309] Department of Defense. Joint Publication 1-02: *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC., 12 April 2001 (as amended through 15 October 2001),145.

[310] Representative Joseph R. Pitts. "Electronic-Warfare Assets Badly Neglected." *National Defense*, June 2000, 39.

[311] In 1988, fiber optic transmission accounted for only 2% of the transoceanic comm. In 2000, that figure had increased to 80% of the market share.

[312] James Adams. *The Next World War*. (New York: Simon and Shuster, 1998,) 96.

[313] Adams, *The Next World War,* 96.

Notes

[314] Linda de Franc. "Ryan Says Space Force Unwarranted For Next 50 Years." *Aerospace Daily* 9 Feb 01, n.p. .On-line. Internet, 18 Jan 2002. Available from http://home.datawest.net/dawog/Space/e20010209space_force_unwarranted.htm.

[315] Joint Publication (JP) 3-33. *Joint Force Capabilities*, 13 October 1999, III-3.

[316] Air Force Doctrine Document 2-2. *Space Operations*, 23 August 1998, 23.

[317] AFDD 2-2, 7.

[318] Ibid, 15.

[319] Ibid, 23.

[320] Ibid, 29.

[321] Ibid, 18.

[322] Ibid, 24.

[323] Ibid, 24.

[324] Ibid, 16.

[325] Department of Defense. *Quadrennial Defense Review Report*. Washington DC: U.S. Government Printing Office, Sep 2001, 45.

[326] Department of Defense Office of General Counsel. *An Assessment of International Legal Issues in Information Operations,* May 1999. On-line. Internet, 10 January 2002. Available http://www.terrorism.com/documents/dod-io-legal.pdf, 30.

[327] Sheila E. Widnall, "The Space and Air Force of the Next Century." Presented at the National Security Forum, Maxwell Air Force Base, AL, 29 May 1997.

[328] Michael Sirak. "USAF Plans 'Space Control." *Jane's Defence Weekly*, 31 Oct 01, n.p. On-line. Internet, 20 December 2002. Available from http://131.84.1.68/Jan2002/e20020108roche.htm.

[329] "Advance Questions for General John P. Jumper Nominee for the Position of Chief of Staff of the United States Air Force," *US Senate Armed Services Committee*, 8 January 2001, n.p. On-line. Internet, 20 February 2002. Available from www.senate.gov/~armed_services/statemnt/2001/a010801jumper.pdf.

[330] Ibid.

[331] Peter Grier. "The Winning Combination of Air & Space." *Air Force Magazine Online.* On-line. Internet, 20 February 2002, n.p.. Available from http://www.afa.org/magazine/Jan2002/0102space.html.

[332] Hap Parker. "Air Force secretary shares views on space road map," *Air Force Link*, 28 November 2001, n.p. On-line. Internet, 20 December 2002. Available from http://www.af.mil/news/Nov2001/n20011128_1691.shtml.

[333] AFDD 2-2, 15.

[334] Ibid, 15.

[335] Dr. Raymond L. Puffer. "The Death of a Satellite," 21 Jun 2001. On-line. Internet, 7 February 2002. Available from www.edwards.af.mil/weekly/docs_html/install-35.html.

[336] Charles Seife. "Where am I?" *Infosec.com*, 19 Mar 2002.. On-line. Internet, 20 December 2002, n.p. Available from http://www.info-sec.com/denial/denial_012298a.html-ssi.

[337] Ibid.

[338] Ibid.

Notes

[339] Jeremy Singer. "Competition Widens But Need for GPS 3 Questioned." Space News, 18 February 2002: 6.

[340] Zalmay M Khalilzad and John P. White. *Strategic Appraisal: The Changing Role of Information In Warfare*. (Santa Monica, CA: RAND Corporation), 1999, 297.

Appendix D

Details of Chapter 4: The Status Quo

> *Officers who are nonconformists often do not advance in their careers because nonconformity in an officer is often confused with counterconformity.*
>
> - Lt Cmdr Anthony Kendall

> *Given the availability of advanced technology and systems to potential adversaries, . . . the United States [will be required] to experiment with revolutionary operational concepts, capabilities, and organizational arrangements and to encourage the development of a culture within the military that embraces innovation and risk-taking.*
>
> - 2001 Quadrennial Defense Review

The Table is repeated for the convenience of the reader and detail follows with respect to Chapter 4's structure.

Table 23: Optimization

“The requirements for that unique expertise are not being fulfilled within the current framework of organization, *or* the resources of that expertise are not being used properly.”[341]	
Primary	**Secondary**
OP1. The AF **appropriately** continues to promulgate kinetic-based weapons over space and/or information weapons	OS1. The QDR recognizes the need for, and calls for, significant transformation
OP2. The AF is becoming more reliant on weapon systems increasingly tied to Information while neglecting Information	OS2. Information Operations requires a new interpretation of Hague Convention and Geneva Convention statutes
OP3. The AF does not have the span of control to prosecute an air war, space war, and information war simultaneously at the strategic, operational, and tactical levels	OS3. AF senior leadership and PME billets are disproportionately allocated with respect to the USAF’s six core tenets
OP4. The DoD’s stagnant division of funding despite new mission areas and a new responsibility calculus fails to support its evolution	OS4. The Air Force has consistently been tied to dogma when it comes to evolutionary concepts
OP5. The Air Force itself remains fractured and tied to its core function of air superiority.	
OP6. The DAL has concluded the AF is not providing the attendant structure required for a future air/space/I-Service	
OP8. DOD has no single organization vested with the responsibility, authority and budget to acquire joint C4ISR systems, at the same time it is requiring increased interoperability.	

Table 24: Uniqueness

<table>
<tr><td colspan="2">“Only an <i>independent</i> [Information] Force can provide a capability that is considered vital to our national defense.”[342]</td></tr>
<tr><th>Primary</th><th>Secondary</th></tr>
<tr><td>EP1: The current military structure is antithetical with respect to the personnel, resources, and ties to industry</td><td>ES1. The other services are incapable of commanding an Information Service</td></tr>
<tr><td>EP2: The current DoD and AF acquisition systems are incompatible with the needs of an Information Service and in fact requires distinct acquisition procedures for Information Systems</td><td>ES2. The Information Service is far more pervasive across all IOPs than is the military IOP, and as such is fundamentally unique. (Proven in Ch 2).</td></tr>
</table>

<u>OP1: Focus on kinetic-based weapons</u>

<u>F-22 Details.</u> The Air Force is pressing ahead with the F-22 program, despite cracks in the tail and in the canopy, and long delays in the 11-year problem, including a two-year delay in testing only lifted by Congress in Aug 01.[343] While these problems are not uncommon in a new aircraft, the cost increase is significant. “Production of all 333 aircraft is expected to cost at least $38 billion.”[344] This is $9 billion over a congressionally imposed cost cap[345] which may cost the Pentagon “85 out of the planned 333 F-22s to stay within congressionally imposed production cost caps.”[346] The cost increases and dwindling number of aircraft the service may buy is enraging some lawmakers. There is speculation the Air Force has determined the program will not succeed under the present cost caps and may seek a waiver, a similar opening move the ill-fated Navy A-6 program tried in the early 1990’s. The Pentagon's independent test office has endorsed the waiver in that the Raptor is “meeting and, in most cases exceeding its key performance requirements.”[347] The F-22 has significant Congressional backing, including Sen. Ted Stevens

(R-Alaska) who stated “We're going to win full restoration of F-22 funding" in response to questions on the F-22 budget battle.[348]

This concentration on fighter aircraft affects not only information and space, but other *aircraft* as well, namely bombers, tankers, EW platforms, and some transports

Bombers. As noted in Table 12, which acknowledges that GO’s with fighter pilot backgrounds outnumber bomber and tanker/transport pilots 4:1 and 3:1 respectively, it appears the Air Force is similarly focused on not only the fighter *pilot*, but the fighter itself. As noted in Chapter 4, the findings are “inconsistent with the findings of the Defense Department’s Long Range Air Power Panel.”[349] Of particular note were the Panel’s conclusions that the Pentagon roadmap:

- “[I]ntegrates a series of **implausibly optimistic** assumptions about future bomber requirements into a report that concludes the current heavy bomber force is probably adequate to meet national needs for the next forty years.[350]
- [P]roposes to spend less than 1% of the Air Force’s investment budget on bomber modernization. [351]
- [P]roposes a series of phased improvements (e.g. radars, navigation equipment, computers, etc.) Welch’s Panel concluded that upgrades begin 30% sooner than suggested[352]
- [A]nticipates new bomber design will begin ~2020, production to begin in 2034 and OIC in 2037. Welch’s panel “anticipated “shortfalls would begin emerging in aircraft numbers and capabilities around 2013, probably requiring new bomber production. The bomber roadmap does not project such problems until over twenty years later.”[353]
- Defers near-term improvements to the B-2 until 2015. Similarly, the Welch panel called for near-term enhancement of B-2 stealth features, whereas the roadmap defers most such work until 2015.[354]

In fact, the differences between the roadmap and the panel are so stark, several prominent Congressional members and retired flag officers conclude it is the result of “bureaucratic politics within the service.”[355] Colonel Robert Chandler (ret) argued that integrating SAC and TAC into ACC “deprived the Air Force of “an adequate forum for planning a rapid-response, long-range bombing campaign and assessing the attendant risks". Chandler's thesis, endorsed by some members of Congress and retired general officers, is that planning for future strike requirements migrated to a community dominated by fighter pilots. This community, which has dominated Air Force leadership since the end of the Cold War, is said to favor tactical aircraft (fighter-bombers such as the F-15E) over heavy bombers for future strike missions.[356] This conclusion is supported by Col (ret) Michael Worden's conclusion in his book *Rise of the Fighter Generals*.

Transports. Other aircraft programs are suffering from the F-22 funding shortfalls as well, in particular, the venerable C-130 Hercules transport. According to Government officials: "The Air Force leadership is debating whether to start buying C-130J transports starting in 2000 instead of 2004 to ensure that production of the Lockheed Martin aircraft remains uninterrupted to avoid increasing costs for the F-22 fighter." The link between the large four-engine C-130J and the stealthy twin-engine F-22 is that both are assembled at Lockheed Martin's massive facility in Marietta, Ga. While production of the F-22 is assured because the effort is the Air Force's top modernization priority--the prospects for C-130J are very different without Air Force participation. One government official noted that "If Lockheed does close the C-130 line until Air Force orders pick up in 2004, there may be upward price pressure on the F-22 as some of the plant overhead attributed to the C-130 migrates to the F-22 program. We want to avoid that."[357]

Tankers. The tanker fleet likewise has been extremely neglected, and now, for the first time appears to have no choice but to lease aircraft from Boeing to meet scheduled obsolescence. "The Senate Appropriations Committee Dec. 4 approved a fiscal 2002 defense spending bill that would allow the Air Force to lease 100 Boeing 767-derivative tankers for 10 years to replace aging KC-135s, whose average age is forty years. Sen.

Daniel Inouye (D-Hawaii), chairman of the Senate Appropriations defense subcommittee, noted “[The KC-135Es] are ready to fall apart."[358] Initial proposals called for a lease-purchase, with the Air Force taking ownership of the planes by the end of the lease.

In an article unrelated to this research, Ms. Darleen Druyun, Principal Deputy to the Assistant Secretary of the Air Force for Acquisition noted, in terms of tankers, “We have a very, very old fleet out there. . . .You reach a point where you have to either completely remanufacture an aircraft or go buy a new one.” Some KC-135 tankers built for Vietnam still are carrying out refueling missions today. And C-5 cargo planes built 30 years ago continue to do the military’s heavy lifting, and B-52’s have been flying for 5 decades.”[359]

Electronic Warfare. Representative Joseph R. Pitts is a USAF combat veteran who flew 116 combat missions as a navigator and electronic warfare officer in a B-52 bomber during three tours in Vietnam,[360] a co-chairman on the U.S. Congress Electronic Warfare Working Group and a member of the Defense Advisory Board at the Lexington Institute.361 “[The] Navy’s EA-6B *Prowler* [is] the Department of Defense’s sole radar support jammer for all the services, including joint air operations.[362] “The EA-6B is the only dedicated tactical-jamming aircraft in the joint inventory, because the Air Force retired its last jammer (the EF-111A Raven) in 1998. . . . [T]here is a spreading conviction among senior Air Force officers, and supported by an internal RAND analyses] that the service made a mistake when it neglected its EW activities to pursue stealth.”[363] Pitts agrees that stealth in its early years was sometimes “oversold as a revolutionary alternative to EW.”[364] As such the Air Force neglected its EW responsibilities and technologies, given stealth’s promise, and “decided--despite the critical importance of EW in Operation Desert Storm--to retire its EF-111 Raven and F-4G Wild Weasel electronic-warfare aircraft." Many factors entered into the decision [to retire the Ravens], including cost, military downsizing, and the new era of stealth aircraft," a decision Pitts agrees "was short-sighted."[365]

Prowlers (Fig. 26) are indispensable in any modern strike package, and they are the only aircraft built primarily to execute "stand-off" Suppression of Enemy Air Defenses (SEAD) EW operations to enable fighter-bomber sorties. While the AC-130 and F-16CJ each employ Electronic Warfare Officers (EWOs) and/or automated EW techniques, the primary SEAD attacks are conducted by the *Prowler*. Unfortunately, "premature force cuts of the EF-111 Raven and F-4G EW aircraft have shifted the sole burden of primary EW onto the *Prowler*, while the acquisition cycle, sustainment budget, and acquisition funds have not kept pace with the increasing need."[366] Pitts further states that the concern is not only with acquisition of a new EW airborne platform, but based on neglect of the current *Prowler* fleet, including "delayed …introduction of new technologies, [including] communications links needed to receive various types of useful data from off board sources such as electronic-intelligence satellites."[367] This statement was confirmed by a resident *Prowler* EWO currently at ACSC.

The *Prowler* has proved indispensable in recent air campaigns such as Operations Northern and Southern Watch to enforce Iraqi no-fly zones, and Operation Allied Force against Yugoslavia. It is rare for U.S. planes to enter hostile air space anywhere in the world without standoff jamming provided by the *Prowler*. Pitts further noted that "[The Kosovo operation] underscored just how neglected EW assets have become."[368] Nighthawks were "supported by the *Prowler*, and the loss of one stealth fighter," which received world-wide coverage and called into question its capabilities both at home and abroad, “was directly attributable to lack of adequate EW coverage.”[369] *Prowler*s were employed in Vietnam, Desert Storm, Kosovo, Yugoslavia, are on patrol today in Operations Northern and Southern Watch, and are a key component of the AFEX and Pegasus wargames scenarios at ACSC.

There were so few EA-6Bs available worldwide to support the Balkan air war that *Prowler*s were shifted out of Northeast Asia and the Persian Gulf region, leaving those areas temporarily uncovered. Pitts added that “The simple truth is that America's airborne electronic-warfare forces are overworked and under-funded,[370] [and] . . .no new airframes have been produced in a decade. The devastating effectiveness of the EW aircraft in Desert Storm was at least in part due to superior intelligence of the Iraqi Integrated Air Defense System (IADS), which may not be the case in the next war. Similar to the Combined Bomber Campaign, the Even the Serbian IADS system, a third-rate military force, had a very robust IADS system.

Figure 26: USN EA-6B Prowler

> "The performance of U.S. forces in Operation Allied Force made clear that Congress and the Pentagon need to pay closer attention to electronic warfare, not just because it is a high-leverage war-fighting skill, **but also because of the strides other nations are making in that arena.** Operation Allied Force . . underscored how critical airborne electronic warfare has become to Western war plans. Serbia's military forces operated an integrated and redundant air-defense system that potentially posed a huge threat to unprotected coalition aircraft. The Balkan air war confirmed several basic lessons about electronic warfare. First, the proliferation of advanced air-defense systems around the world has severely compromised the survivability of nonstealthy aircraft unless they receive continuous EW protection in combat. **Second, stealth and EW are complementary, especially when jamming is provided by standoff platforms to stealthy penetrators that themselves emit no signals.** Third, because EW support is important for both stealthy and nonstealthy aircraft, the military needs a bigger force of airborne jammers than anticipated only a few years ago. In short, Operation Allied Force proved that, at least in the case of electronic-warfare aircraft, the United States did not have the capacity to prosecute two major theater wars simultaneously [emphasis added]."[371]

Together with the authors of JV2010, **Pitts agrees that EW is at least a form, if not a subset of Information Operations.** Pitts writes:

> "For a variety of bureaucratic and doctrinal reasons, the armed services today prefer to differentiate electronic and information warfare. But from **a purely practical perspective, it is obvious that EW has always been about controlling the electromagnetic spectrum in wartime** so that we can know the enemy better than he knows us." He goes on say that "low observables (stealth) are just one in a series of measures conceived to preserve electromagnetic dominance."[372]

<u>OP2: Increased reliance on weapon systems requiring Information Dominance .</u>

<u>Unmanned Aerial Vehicles.</u> UAVs will play a significant role in all future airpower operations, as noted by Major Butler

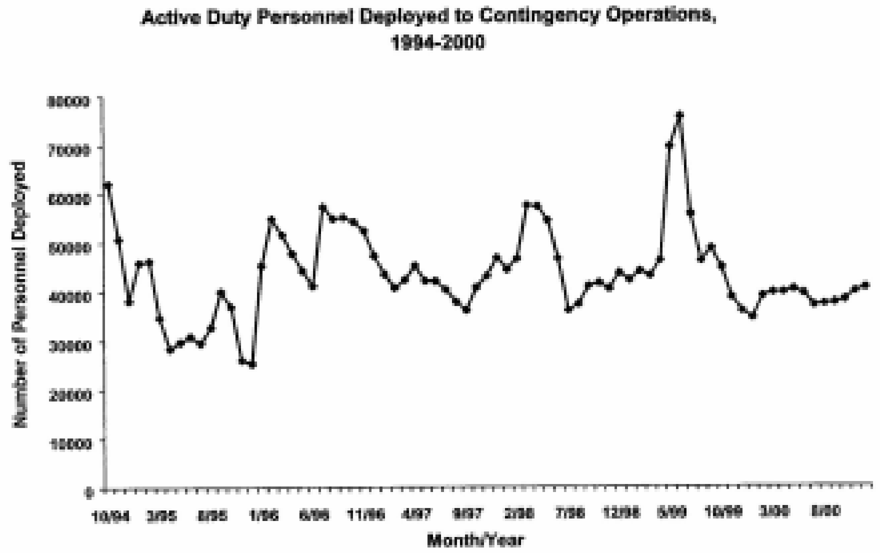
> "Unmanned (or uninhabited) aerial vehicles (UAVs) are methodically becoming a central theme in the mosaic of Air Force systems and capability. The questions regarding employment of UAVs are not so much about if they should be developed but how to integrate them into Air Force doctrine and organizations."[373]

The QDR strongly endorsed UAVs as well, noting "Efforts are underway to accelerate the procurement of additional Unmanned Aerial Vehicle (UAV) platforms," including SIGINT payloads.[374] In addition, ISR will be the centerpiece of military reforms triggered by operations in Afghanistan. Secretary Rumsfeld "predicted that UAVs and communications links (that tie together UAVs, combat aircraft, bombers, ground controllers and smart munitions) will emerge as the two items of most value in the war in Afghanistan, [noting their] very powerful effect."[375]

Maj Butler's explains the focus on UAVs with the following:

1. - "Gen Jumper, then ACC/CC, "[pointed] to ISR UAVs as an essential element of the Global Strike Task Force concept designed to maximize the effectiveness of the future Air Force."[376]
2. - "The Air Force has recognized the growing value of ISR for expeditionary operations and concluded that the marriage of UAVs and advanced sensors provides improved air power capability for the future."[377]
3. - "US operations in the Balkans have substantiated the ability of UAVs to provide timely ISR to military commanders. As the workhorse UAV, the *Predator* has logged over 20,000 hours and made several combat deployments to the Balkans."[378]
4. - "The *Predator*, in concert with other UAVs and ISR collection platforms, provided invaluable real-time intelligence. The *Predator* has electro-optic (EO), infrared (IR), and radar sensors that allow day/night operation in all weather. The *Predator* can transmit imagery through its line-of-sight radio or over the horizon using a satellite link."[379]

UAVs are performing tremendously in OEF, including multiple UAVs being commanded from a single command post, and "accumulating a nearly 100% record of hits."[380] And while the press still concentrates on accidental or combat losses, the fact of the matter is that only hardware is lost--particularly critical in the politically sensitive world of espionage (EP-3 incident), and the media's increasing attention on combat deaths. While various studies clearly show America is not as *adverse* as suggested to combat fatalities in those cases where the combat action is deemed vital to American interests, the nation as a whole is still incredible sensitized nonetheless with the media daily tallying losses (e.g. accidental losses, combat losses, friendly fire losses, losses of UAVs losses of $100M stealth aircraft, etc.), and following the casket of a single soldier and their distraught family for weeks. These type of operations will only increase as the international environment, no longer constrained by two dichotomous ideologies, further fractionates as it painfully transforms itself from a unipolar to a multipolar construct. This trend is graphically portrayed in Fig. 27.



Source: 2001 QDR, 59.

Figure 27: Active Duty Deployments Sharply Increase (Note: Pre-9/11)

The QDR likewise directed that "emphasis must be placed on manned and unmanned long-range precision strike assets . . ." and for DoD to increase procurement of "unmanned combat aerial vehicles and intelligence, surveillance, and reconnaissance unmanned aerial vehicles such as Global Hawk."[381] Impressed by Global Hawk's potential, Secretary Rumsfeld drastically accelerated the further incorporation of *Global Hawk* into the Air Force inventory. Block 10 versions were moved forward five years--from 2009 to 2004, and he increased acquisition 300%--from two/year to six/year.[382] The *Predator*s are receiving the same kind of acceleration. *Predator*s acquisition will increase 350%, from seven/year to 24/year.[383]

Stealthy UAVs “snagged the SECDEF’s attention”[384] after the EP-3E loss, which some consider a black-eye on American foreign policy. The leading option, “on how to avoid future embarrassing and damaging losses of classified equipment, documents or aircrews to midair collisions, attacks and capture,”[385] centers on starting a new, stealthy UAV reconnaissance program that would field 12-24 aircraft. *Darkstar*, the original concept, was terminated in that it did not possess the payload, range and degree of stealth a future UAV required, and the USAFD did not have the budget for it. (There is widespread speculation as well that the fighter-dominated leadership was uneasy with the craft’s significant self-sufficiency.) The new Stealth UAV program would cost “around $1.5 billion in new money to develop, . . . and would cost as much as “$200 million each equipped with a 1-1.5-ton payload, to fly at 75,000 ft.”[386] Another factor that increases costs for a covert, virtually invisible UAV, would be communications links. "The Global Hawk UAV is not stealthy so it can use UHF communications satellites, and everybody knows it's there."[387] But UHF has tremendously low bandwidth (i.e. it can’t relay much information.) Future UAVS may carry an improved LPI SAR, electro-optical/infrared video and more importantly, a signals intelligence-gathering package, or active electronically scanned array radar (AESA). AESA can execute in either an active or passive mode, collect and jam simultaneously, and can control its own side-lobes to defeat enemy radar. The key to LPI is operating in a multiple-bi-static mode where “One pulse of radar is emitted by the first aircraft, a second by a supporting UAV, and both are fused and refined with satellite-based radar observations.”[388] **Again, this new UAV is critically de-**

pendent on interoperable C4I systems and both land-based and SATCOM data links and communications, and exploitation of the EM spectrum.

UAVs and decoys are crucial elements in the Air Force's information attack plans, which are slated to achieve an operational capability by 2010. Papers being briefed in the Pentagon call for "penetrating, close-in and standoff [operations] by unmanned, multi-spectral electronic attack platforms." The weapons or "tools" to be employed include radio frequency jamming (an AESA capability), directed energy (lasers can be used to jam or, at higher power, damage infrared sensors or electronic circuitry), or high power microwaves (that produce destructive spikes of energy in electronic devices). [389] In addition, UAVs have some inherent advantages and thus are more attractive for an increasing number of *appropriate* missions:

1. - According to John Stenbit, the Pentagon's C3I chief, UAVs provide “persistence"--the value of long-term surveillance compared with short-term reconnaissance.” [390]
2. - UAVs also can get closer to a target to pick up low-power signals, without endangering aircrews.
3. - Finally, UAVs are much cheaper than the alternatives. intelligence from space, has grown increasingly difficult and expensive. Employing more UAVs into the mix would provide impressive synergy--the space systems providing broad view and cueing UAVs to move in for closer looks before the satellite returns in 100-110 minutes. Current UAVs can loiter over the battlefield from 8-24 hr. at a time, and others are in development that could stay aloft for weeks relaying faint signals from the battlefield.

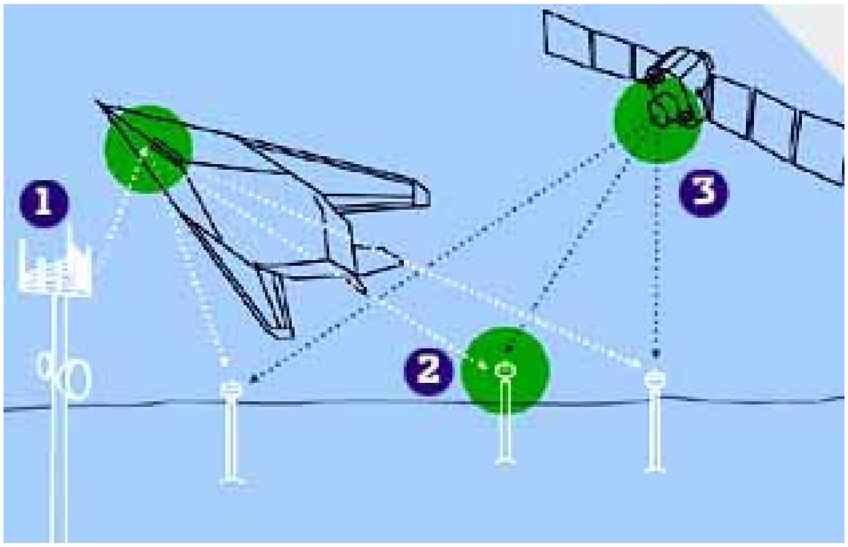
But at the same time, UAVs are critically dependent on communication links, many from SATCOM, which can be easily jammed. UAVs communicate via Intelsat’s Telstar, which is not secure. In addition, UAV comm is carried over consortium satellites, meaning the US or its allies may be dependent on those very satellites for its own links. UAVs use a myriad of comms during employment. The RQ-4, *Global Hawk* (GH) and RQ-1, *Predator* use Ku-band Commercial Satellite Communications

(SATCOM) to download their sensor data to ground stations. GH uses UHF SATCOM to maintain a command and control (C2) tether beyond-line-of-site (BLOS). GH uses Common Data Link (CDL) for LOS data download and UHF for C2 tether. *Predator* uses a LOS C-band link for data download and C2 tether.[391] There *are* problems with the communications systems on the UAVs. The GH Command and Control, Computers and Communications, Intelligence Support Plan (C4ISP) lists over 20 shortfalls, most without funding for identified solutions.[392] Units are beginning to realize that most of the operation and maintenance for the Ground Control Station (GCS) is communications-related.

Precision Guided Munitions (PGMs)

The Air Force, and the DoD as a whole, are increasingly reliant on PGMs. In fact, 73% of the munitions dropped in OEF are PGMs.[393] "The emphasis on precision-guided weapons is a big change from the mid 1970's. General Myers, the former Chairman of the Joint Chiefs of Staff, recalls that precision targeting techniques weren't a high priority for most flyers noting that the "places to be in the Weapons School was the air-to-air and air-to-ground flights."[394] A such, the Air Force has allowed its inventory of video-guided Mavericks to dwindle as Joint Direct Attack Munitions (JADM)[395] and Joint Air-to-Surface Standoff Missile (JSASSM) fill the inventory. Both rely on GPS, although JASSM is purported to have un upgraded anti-jam electronics suite.

Stealth. Siemens, one of the world's largest corporations and headquartered in Germany, reported that one of its small research firms, Roke Manor Research, had "rendered stealth aircraft useless" by employing cell phone emissions in a passive radar net exploiting the tenets of bi-static radar.[396] Roke engineers noted they could "[not only] detect the plane but also to determine its exact location."[397] Like cold fusion, their theory has not yet been proven, nor do they have a working prototype. Their brassboard design, "now the size of a sport-utility vehicle but soon to be the size of a briefcase,"[398] likewise requires enormous amounts of computing power, power that while not yet available can be in a mobile platform in 5-8 years, given Moore's Law, or take advantage of the Howard Cascade (Fig. 29), being developed to economize the commercial satellite imagery market.



"The detection system developed by Roke Manor -- passive bistatic radar -- uses an existing cellphone tower as its transmitter. 1. Ordinary cellphone signals bounce off stealth plane. 2. Receivers collect cell-phone signals and their echoes. 3. GPS satellite signals are used to synchronize the receivers. Computers then sift the data to detect spy craft. (Illustration by: Stephen Rountree)."[399]

Figure 28: Potential Stealth Detection via Passive Cell-Phone Network

Particularly sordid is the system reliance on the US's own GPS signals[400] to synchronize the multiple receivers, and cell phone signals--possibly DoD signals--to provide the radar signal, in that the bi-static system is passive--it relies on no signals of its own as in conventional radar. That means it's harder to hit kinetically because an anti-radiation missile can't home in on it, and the system is widely dispersed. It also means the pilot will no longer know the bomber has been illuminated. The Air Forces denies the Roke reports holds merit, but conceded bi-static radar holds promise, and appears to be building their own airborne bi-static radar system.

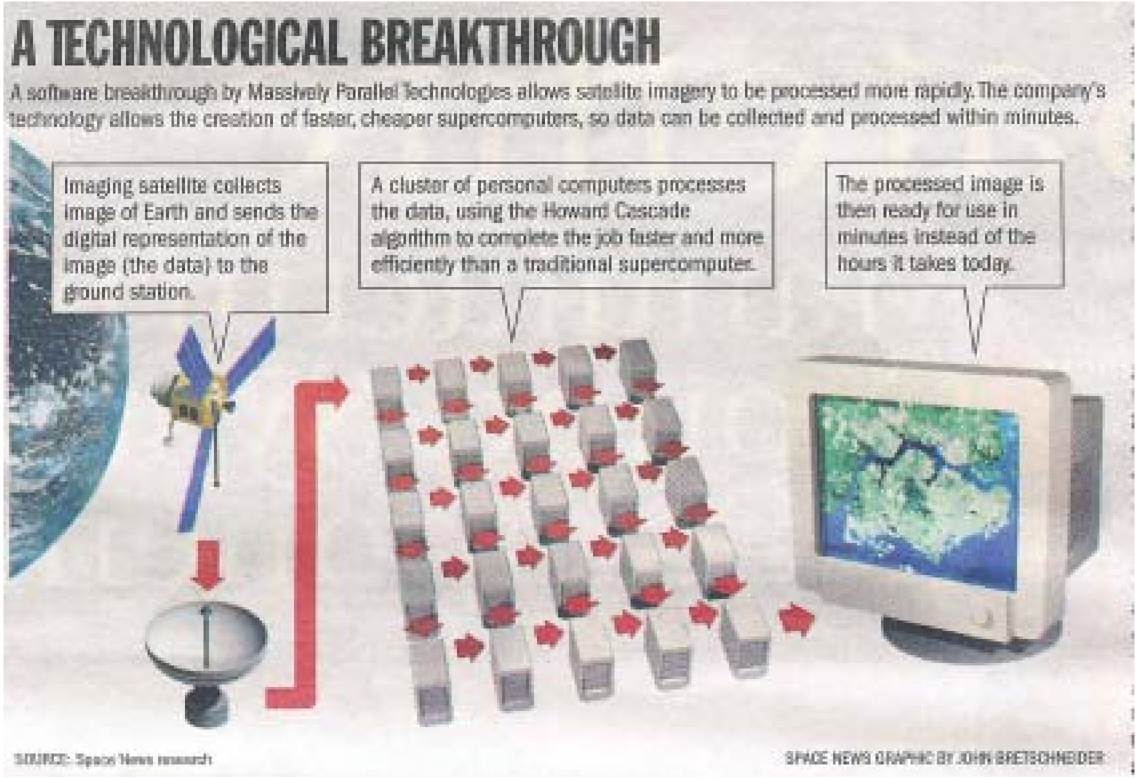

A TECHNOLOGICAL BREAKTHROUGH
A software breakthrough by Massively Parallel Technologies allows satellite imagery to be processed more rapidly. The company's technology allows the creation of faster, cheaper supercomputers, so data can be collected and processed within minutes.
Imaging satellite collects image of Earth and sends the digital representation of the image (the data) to the ground station.
A cluster of personal computers processes the data, using the Howard Cascade algorithm to complete the job faster and more efficiently than a traditional supercomputer.
The processed image is then ready for use in minutes instead of the hours it takes today.
SOURCE: Space News research
SPACE NEWS GRAPHIC BY JOHN BRETSCHNEIDER

Figure 29: Howard Cascade Can Provide Supercomputer Power at Fraction of Cost (and leaving virtually no audit trail)[401]

Popular Science's sources spotted a T-43 Radar Test Bed (RTB), a modified 737, which appears to have been modified to carry a bi-static radar system. That it carries a bi-static radar system is supported by four factors: 1) body configuration, (the shape and size of the nose and tail radomes-6.5 feet in diameter suggest they contain moving antennas); 2) the RTB's R&D work is being conducted by Denmar Corporation, which specializes in stealth technology and was founded by former Skunk Works engineer, Denys Overholser, who worked on *Have Blue*, the Air Force first Stealth aircraft; 3) Technical papers from Rome Lab, which include a "graphic in a Lincoln Lab briefing paper [showing] a bi-static radar with its transmitter mounted on a 737;"[402] and 4) new stealth designs are, perhaps coincidently, being designed with materials to absorb and re-channel the microwave frequencies used by cellphones.[403]

Stealth aircraft, like the F-117 *Nighthawk* and B-2 *Spirit* absorb[404] and or reflect[405] radar signals--basically "they are very bad antennas that are then made to fly."[406] However, both were designed based on the assumptions that went into *Have Blue*'s designs--namely predicated on the threat of *homeostatic* radar. Bi-static radar systems pick up the deflected signals, and computers with location data from GPS satellites, can decouple the signals analytically determining range. Ranging is far more difficult in the bi-static system and likewise requires massive computational power. It is appropriately ironic as well--the radar system first used in London in 1940 to counter the Luftwaffe used the BBC's main transmitter in London to illuminate the target.[407]

Likewise, while Pentagon official dismissed Rake's claims that they can defeat the stealth systems, they did note that other potential passive bi-static systems, could work. These systems rely on a passive net formed by radio and television signals (which have much greater power than cell phones but far less than the active radar system comprising most IADS systems and likewise suffer the same dispersion effects). Lockheed's *Silent Sentry* system, which employs these effects, does "have some potential against stealth targets."[408] Stealth *is* improving. For example, stealth is easily defeated by a simple element--they are highly visible in daylight. As such, they were only able to fly in Desert Storm and ODF at night. "In recent Air Force tests, however, a B-2 with upgraded stealth was able to fly between an F-15 and F-16 operating about 20 mi. apart without being seen visually or electronically."[409]**As noted above, Stealth is just the countermeasure to EW and vice versa, and EW is Information Operations.** While it is not the intent that an I-Service would acquire and/or operate stealth aircraft, the synergy cannot be ignored and a single service can best coalesce the offensive and defensive sides of EW and stealth across services and across platforms.

C4ISR. Reachback has become increasingly critical as forces continue to drawdown and industry increasingly assumes the mantle to provide support services. Reachback allows a smaller footprint into theater, reducing stress on transport and basing rights. Secure, high bandwidth SATCOM will only grow more critical as Reachback is critically dependent on it and communication in general. Keith Hall noted the contribution in recent testimony before Congress: "The global presence of space systems makes it possible for the U.S. to more effectively respond to the wide range of threats presented by the post-Cold War world. [OAF was a notable success story for 'Reachback.'] Relying on satellite communications, warfighters were able to reach back to the United States for real-time information and analysis (some of that space based, as well), while avoiding the need to deploy in-theater systems."[410]

Gen Myers, then USSPACECOM/CC likewise noted the contribution of Reachback during the 1998 Expeditionary Air Force Exercise (EFX98), extrapolating lessons learned to the associated 2004 scenario: "Because space systems enable reachback concepts, the Air Force was able to deploy more combat teeth to the fight by leaving more of the support tail here at home."[411]

MILSATCOM will remain critical. In Desert Storm, "Satellite communication was the backbone of long-haul and intra-theater connectivity for the Gulf War. Over 90 percent of the communications into and out of theater went over communications satellites.

Almost one-quarter of all satellite communications traffic was carried by commercial systems."[412] This dependence has already grown to 95%, as noted in the following:

> "Advances in information technologies have resulted in the proliferation of advanced AIS on which JFCs are critically dependent for the conduct of joint operations. Additionally, such information systems are ubiquitous in the public and private sectors, and comprise the inextricable backbone of many critical infrastructures such as power and water, as well as information infrastructures like television, satellite communications, and telecommunications, all of which may support JFCs operations. For example, 95% of DOD communications are supported by commercial information infrastructures[413]. Thus, while defensive IO are limited to protecting information systems and information infrastructures, those information infrastructures are inextricably linked to larger considerations of protecting other critical infrastructures, and to the larger issue of homeland defense. The integration of automated information systems in all types of supporting infrastructures requires us to reshape our thinking in terms of the level and extent of protection such systems require to ensure effective joint force protection and operations."[414]

Meanwhile, the civilian community is migrating more to fiber optics, which, like civilian-based SATCOM, is not secure.

In addition, the Air Force is strongly considering integrating ISR assets on many of its larger airframes, namely tankers and transports. Integrating these systems, as individual intelligence assets or as relay points for UAVs, ground, and space-based systems requires not only a new commitment for the air-breathing community, but a vast architecting load on the C4ISR infrastructure, one which demands flexibility, modularity, and rapid action. Again, C4ISR is becoming more and more critical.

OP3: The Air Force does not have the requisite span of control.

As noted in Table 11 in this Annex's parent chapter (Chapter 4), the Air Force's roles are increasing dramatically with no commensurate increase in relative budget authority. Yet. the DoD has no intention of separating the space or I-Services. Fall CORONA 2001 made enormous strides in recognizing the difference between the air and space mediums, in noting that the term “Aerospace” a terms coined in the early 90’s to show the two mediums as indistinguishable, will gradually be replaced with the term “Air and Space.” Yet it refused to accept the instantiation of either a Joint Forces Space Component Commander or Joint Forces Information Component Commander. In addition, former CSAF General (ret) Michael Ryan agrees the time for a separate space force is far away, noting “there is no need for a Space Force or Corps separate from the USAF until mankind moves beyond the earth's orbit - likely at least 50 years away. . . . But it will come.”[415] One such area which is increasing dramatically, is the area of space control. The magnitude of change is dramatic as noted in a recent article by Allen Frye, a political scientist chosen and Congressional Fellow of the American Political Science Association:

> “Among the many skirmishes in connection with the . . . Administration’s budget proposals . . .over the national space program seems likely to grow into a major political battle. The civilian space agency's program, for which the President is asking “[$31][416] billion (an increase of $[11][417] billion), has come under unprecedented congressional scrutiny. Meanwhile, sentiment is building up on Capitol Hill for a more substantial military space effort. . . .Congress has always shown a special concern for the military implications of space activities. A common feature of these and other systems which the Defense Department is thought to be developing is that **none of the devices are weapons**. The non-weapon character of American military satellites is the basis for our continued insistence that the United States space program is fully compatible with the reservation of space for peaceful purposes. **There appears to be no United States effort to develop a space-based force of bombardment satellites or other weapons**. The consistent threats to paralyze United States reconnaissance and surveillance satellites suggest that the Soviets may indeed be seriously engaged in devising a satellite interceptor and that they are very likely to use it, [a program they have been working since 1963 [See Appendix ?]]. In negotiations regarding space the United States has already given the Russians the very prize for which we propose to negotiate. The Soviets enjoy adequate security that the United States will not use space for deployment of weapons, while the United States has no comparable guarantees from the Soviets. From Moscow's point of view, there is no need to negotiate in earnest for arms control in space. A vital question for American policy makers in the months ahead is whether we are committing the same mistake in negotiations concerning space. Indeed, current political and

> technical trends make it seem more likely that the Russians will regard space weapons as highly advantageous, both politically and militarily. .”[418] [emphasis added]

This is in line with the Secretary’s QDR where the need for space control pervades the document as indicated in this telling passage directing the DoD to

> “Enhance the capability and survivability of space systems. Because many activities conducted in space are critical to America's national security and economic well being, the ability of the United States to access and utilize space is a vital national security interest. During crisis or conflict, potential adversaries may target U.S., allied, and commercial space assets as an asymmetric means of countering or reducing U.S. military operational effectiveness, intelligence capabilities, economic and societal stability, and national will. Ensuring the freedom of access to space and protecting U.S. national security interests in space are priorities for the [DoD].”[419]

The key difference is that Frye’s article was written in 1963 (and the author apologizes for taking liberty with use “recently”), 40 years before Rumsfeld completed the QDR; i.e. **this is an enormous task**, a completely new mission area, and the USSR, now collaborating with the Chinese on space control, have been doing it for forty years, as shown in Table 24.

Table 25: USSR ASAT History[420]

Cat #	Int'l designator	Name	Launch date	Incl.	Remarks
683	**1963-043A**	Polyot-1	1-Nov-63	58.92	Interceptor engine test. Initial: 339-592 km
783	1964-019A	Polyot-2	12-Apr-64	58.06	Interceptor engine test. Initial: 242-485 km, 59.92 deg
3013	1967-104A	Kos-185	27-Oct-67	64.09	Test of interceptor engine only.
3216	1968-036A	Kos-217	24-Apr-68	62.2	Injection into final orbit failed
3503	1968-090A	Kos-248	19-Oct-68	62.25	
3504	1968-091A	Kos-249	20-Oct-68	62.33	Intermed orbits:105-138 km, 502-1639 km
3530	1968-097A	Kos-252	1-Nov-68	62.32	
4058	1969-066A	Kos-291	6-Aug-69	62.24	Wrong target orbit due to engine failure
4590	1970-087A	Kos-373	20-Oct-70	62.93	Target orbit raised slightly after 1 w.
4594	1970-089A	Kos-374	22-Oct-70	62.96	Initial orbit:530-1053 km
4598	1970-091A	Kos-375	30-Oct-70	62.8	Initial orbit: 566-994 km
4922	1971-010A	Kos-394	9-Feb-71	65.84	New, smaller, type of target.

Table 24 (Cont.): USSR ASAT History

Cat #	Int'l designator	Name	Launch date	Incl.	Remarks
4964	1971-015A	Kos-397	25-Feb-71	65.76	
5050	1971-020A	Kos-400	19-Mar-71	65.85	First attack from below
5113	1971-027A	Kos-404	4-Apr-71	65.74	Moved to 169-799 km after approach
5625	1971-102A	Kos-459	29-Nov-71	65.83	
5646	1971-106A	Kos-462	3-Dec-71	65.88	
6206	1972-074A	Kos-521	29-Sep-72	65.89	Target. TM system failed. (5)
8688	1976-014A	Kos-803	12-Feb-76	65.85	New IS-P target (5)
8694	**1976-015A**	**Kos-804**	**16-Feb-76**	**65.75**	**"Rendezvoused" with the target**
8806	1976-034A	Kos-814	13-Apr-76	65.07	No intercept orbit available
9011	1976-067A	Kos-839	9-Jul-76	65.86	
9043	1976-071A	Kos-843	21-Jul-76	65.11	No intercept orbit available
9601	1976-120A	Kos-880	9-Dec-76	65.85	Similar orbit to Kos 394
9634	1976-126A	Kos-886	27-Dec-76	65.84	Intermed. orbit 533-1267 km
10010	1977-036A	Kos-909	19-May-77	65.87	Very similar to Kos 839
10014	1977-037A	Kos-910	28-May-77	65.1	No intercept orbit available. Rocket orbit given here.
10065	1977-050A	Kos-918	17-Jun-77	65.11	No intercept orbit available.
10419	1977-101A	Kos-959	21-Oct-77	65.84	
10434	1977-104A	Kos-961	26-Oct-77	66	Intercept orbit not confirmed. Initial: 125-302 km.
10512	1977-116A	Kos-967	13-Dec-77	65.83	
10531	1977-121A	Kos-970	21-Dec-77	65.85	Interm. orbit 158-744 km, 65.1 deg
10904	1978-050A	Kos-1009	19-May-78	65.87	Another "slow" approach
11750	1980-026A	Kos-1171	3-Apr-80	65.84	
11765	1980-030A	Kos-1174	18-Apr-80	65.83	Initial: 124-340 km, 65.1;After: 380-1660, 66.1
12149	1981-006A	Kos-1241	21-Jan-81	65.82	
12160	1981-010A	Kos-1243	2-Feb-81	65.82	Explosive charge failed.
12337	1981-024A	Kos-1258	14-Mar-81	65.82	
13259	1982-055A	Kos-1375	6-Jun-82	65.84	
13281	1982-060A	Kos-1379	18-Jun-82	65.84	NOTE: K=Kosmos

OP5: The Air Force itself remains fractured

James Smith: In 1997, the USAF directed its Institute for National Security Studies (INSS) to ascertain and analyze the reality of the cohesion problem, and if applicable, recommend changes. It's findings were harsh, but hopeful. The study noted: "

> "Today's Air Force has a cohesion problem. The Strategic Air Command (SAC) and Tactical Air Command (TAC) have gone away, melding into Air Combat Command (ACC), but you still hear "fighter wonks" and "bomber weenies" deride each other. You hear pilots bad-mouth navigators (and vice versa), and what is this with a distinctive blue "flight" suit for the "missile pukes?" You don't even want to hear what the non-rated folks have to say about the "leather jacket brigade!" Or what the "near earth air force" has to say about the "pigs in space." **And what about the "computer geeks" and those "airhead engineers?"** Overstated? Perhaps. But there have been graphic examples of each of these internal United States Air Force (USAF) divisions over recent years. Indeed, the Air Force has a cohesion problem, and **it is firmly rooted in Air Force culture, subcultures, and organizational dynamics** within the diverse, complex entity that is today's USAF [emphasis added.]"[421]

The INSS study, although executed in 1997, did not look at the field of information operations at all. It did, however, note the most significant cause of lack of cohesion was technology, particularly between air and space, and the military utility of the latter. The study supports this conclusion, noting that:

> "An initial profile of USAF officers points to a continuation and perhaps even a deepening of some of the factors seen as contributing to USAF occupational orientation and fragmentation. A primary indicator of continuing USAF attachment [is] to technology . . ."[422]

This lack of cohesion was not only apparent to Carl Builder, but to two Secretaries of the Air Force (Drs. Donald B. Rice and Sheila Windall), and to a number of organizational experts, including Dr. Earl Walker, LtCol Franklin Margiotta, and Arnold Kanter, an expert on military organizations across the DoD.

Carl Builder characterizes the contemporary USAF as lacking any integrating vision noting fractionalization with the space faction now heading off on its own toward a separate force future. He sees attachment to

> "technologies without any glue to bind those technologies together around traditional roles and missions of airpower, with the result a dominance of occupationalism over institutional attachments. To Builder, the USAF has no strong, unifying mission or vision, so loyalty has devolved to functions, technologies, and occupations."[423]

Dr. Earl Walker credits organizational culture and the core mission of that culture as the driving impetus. But while giving the culture a sense of identity, any subculture outside of that culture is found to be antithetical and as such

> "the dominant culture pushes out, or rejects accepting, non-core missions as possible detractions from its core focus [and] favor[s] policies that promote the core mission."[424] He further asserts that "true organizational change requires a cultural transformation--not simply accommodation and incremental modification but changed organizational output in terms of structure, professional incentives, and changed professional behaviors. Incremental modifications fail to keep pace with changes in the organization's task environment . . ."[425]

Margiotta agrees, stating in his experience he served in or with 30-40 different "air forces," with the only common elements between them a single colored uniform and a universal belief that each member and faction was serving the cause of the national defense.[426] Dr. Arnold Kanter's research pointed to the differences among service cultures and cohesion. He found:

1. - The Army is the "most closely integrated service, [attributing its cohesion to . integration and mobility across one's career, branches, and bases, which traditionally have several core functions. In the Air Force, we have acquisition bases (Wright-Patterson, Los Angeles AFB, and Hansom AFB; technology bases, Kirtland AFB, Rome Laboratories, and Wright-Patterson AFB, and fighter bases. Army bases are not designed that way--all elements are integrated because all elements fight as an integrated team. [427]
2. - The Navy to be "the second most cohesive of the three largest services" in that it too is a highly interdependent operational organization, crating a "binding force across weapons systems and specialties . . ."[428]

3. - The USAF was the "least cohesive of the services." Kanter attributed this lack of cohesion to specialized technologies and relative isolation of its core specialties, as noted in sub-bullet one, among other things. He too puts the onus on technology, and the lack of a deployable, interoperable team.[429]

The Air Force has consistently been tied to dogma when it comes to evolutionary concepts

Each time a new revolution took place that seemed to threaten the Air Force's devotion to the Airplane, the USAF rejected it, it was developed by its sister services, and the Air Force, then took it as its own. This is the case in ballistic missile technology, initiated by the US Army, and space, likewise initiated by the Army. It is also the case with UAVs, originally dismissed by the Air Force, and programs cancelled only to be matured first by the USA and then by the US Navy and retaken by the Air Force once they saw that they could not deny the utility UAVs afforded. Likewise, the Air Force became fixated on the Space Transportation System to ferry its military satellites, all but abandoning unmanned launch vehicles. LtCol Jimmy Morrell, then in HQ AF planning division, put his career on the line to insist on the continued development of unmanned launch vehicles. When the space shuttle *Challenger* was destroyed on 28 January 1986, and subsequently grounded, again the Air Force was struck with the impact of its own narrow-minded policies. With no launch vehicle to launch the DSCS III satellites, carrying the overwhelming majority of both non-secure and secure MILSATCOM, the DSCS constellation rapidly deteriorated to half its on-orbit constellation coverage. At the onset of Desert Storm, AFPSC actually had to move a lower capacity, less secure DSCS II satellite over 100 degrees over 45 days to cover the communications gaps.

The Infosphere is truly unique

Chapter 2 clearly proved the extent of the threat. Tenets of structural realism clearly dictate that when the power balance is upset, nations engage to restore that balance. The threat is real and demonstrated--yet the DoD has not marshaled a single executive agent to counter this threat, but instead has dispersed them. Yet information is the only asset that:

- Pervades every action the military executes
- Affects the average American on a daily basis
- Pervades every instrument of national power--including economic, political, military, and informational
- Has no concentration of mass (e.g. the Army has the majority of land forces, the Navy the majority of sea forces, and the Air Force, the majority of air forces.)
- Has acquisition procedures completely separate from that of every other item procured by the services
- Has spurred its own "age" akin to the Industrial Age
- Has the same characteristics, changing only in type and magnitude, in all mediums,--air, land, space, sub-surface
- Is The single pervasive element of Joint Vision 2020

In addition, Information, traditionally information-in-warfare, is far more pervasive than any other military force. All other IOPs are dependent on it, as it is on them. Technology, like science, cannot be bounded--our strength as a country is innovation underpinned by capitalism. Engineers turn science into practical end-products. Information is the practical end-product. Technology, like science, cannot and should not be bounded except by the ethical nature of the nation.

Every other service has kinetic, force-on-force, largely symmetric, weapons. The Air Force has long been criticized as to the fact that the majority of its people, 82% in fact, are involved in support roles. In the USMC, every Marine is a rifleman. In the Army, the overwhelming majority are part of a combined arms team, and virtually every officer will at one time command a unit. In the Navy, a smaller majority are involved in operations and the majority serve 30-50% of their careers at sea. The Air Force is unique in that regard, despite its role in strategic bombing, air superiority, and ground support.

The I-Service would have no such kinetic weapons, although it would possess forces that can generate a range of effects up to and including those caused by traditional kinetic weapons. Instead, the I-Service would provide information weapons specialists to the combatant commander. As Secretary Rumsfeld said: "We're so conditioned as a people to think that a military campaign has to be cruise missiles and television images of air-planes dropping bombs and that's just false."[430] Information Warriors understand their unique contributions. The problem is not to build stove-piped information warriors, but to cross-train kinetic warriors in the art of IO. An F-15E pilot understands EW, and EW is a subset of IO. An Information Warrior will never be a decisive force in the same way the USN, USA and USAF can. But it can strategically paralyze the adversary, save the lives of Americans, coalition partners, and even the adversary. And a single service would finally achieve the unity of action necessary to acquire and coalesce the myriad, disparate and incompatible C4ISR systems. C4ISR procurements have been stove-piped by service, by area, by function, by geographic domain, by classification, by degree of military worth, and unfortunately by several of these characterizations simultaneously. The DoD no longer has the luxury of multiple C2 centers.

In addition, the current services were birthed in traditional Euclidean space--land, sea, then air, and recently space. That structure cannot cover the Infosphere in that the Infosphere, unlike tanks, fighter aircraft, submarines, satellites, and military personnel does not occupy Euclidian space.

EP2: The I-Service is incompatible with DoD and USAF acquisition procedures. The DoD has already set a key precedent for the need for a separate service by providing a different path for acquiring information systems in two regards: 1) Separate acquisition standards and guidelines, and 2) the Interoperability Critical Performance Parameter (KPP) that pervades every DoD acquisition.

The DoD acquisition system breaks acquisitions down into four categories with respect to the magnitude of the program. One would think that purchasing food, vice manpower, services, and carriers would be inherently different. This is not the case--the differences come in the details on contract type and method, but never magnitude. Information systems, however, are inherently different, requiring different thresholds, oversight, approval mechanisms, and even separate criteria. Instructors at the Defense Systems Management College, DoD's top acquisition school for training acquisition officers from all services to better understand acquisition principles, speculated that the division between MAPS and MAIS was due in part to DoD's inability to acquire information systems based on their inability "to think outside of the box--NSS's are a wholly different animal" that do not play by the rules.[431]

This thought is further supported by General Linhard, former CSAF assistant for long-range plans. "One of General Linhard's biggest concerns is that the acquisition system is running too slowly to keep up with the threats engendered by IW . . the cycle time for a generation of computers is months, while the cycle time for our acquisition system is much longer. He stated that "we must find a way to integrate the state of the art in some timely fashion."[432] Nor is this likely to change. Systems have obeyed Moore's law for two decades and shows an increasing, not decreasing rate. Early airpower advocates were in the same dilemma--the field was so new during the interwar period, that it was difficult to mass-produce aircraft that would not become immediately obsolete. This technological acceleration and French Ministry of Defense's attempt to beat it, resulted in a devastating acquisition technique called “la politique des prototypes,” the policy of the prototypes.[433] That leadership could not agree as to what airpower role it needed, was epitomized by this prototype procurement strategy which contracted for small numbers of aircraft, and constantly shifted its focus. This strategy not only resulted in a disparate air force composed of obsolete aircraft, it also failed to provide the requisite capitol to develop a national infrastructure capable of mass production. The problem was that aircraft technology was developing faster than evolution in the procurement process, and could not be impeded by procurement boxes. The DoD cannot afford to do the same with Information.

DoDI 5000.2 “Operation of the Defense Acquisition System” defines an Automated Information System[434] as “An acquisition program that acquires Information Technology (IT), except IT that: . . . Involves equipment that is an integral part of a weapon or weapons system; or . . .Is a tactical communication system.” It further defines a National Security System (NSS) as “Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which: Involves intelligence activities; . . . Involves cryptologic activities related to national security; . . .Involves command and control of military forces; . . .Involves equipment that is an integral part of a weapon or weapons system[435] All NSS programs therefore are AIS programs. However, MAISs do not include highly sensitive classified programs (as determined by the Secretary of Defense) or tactical communication systems.

DoD 5000-2R, *Mandatory Procedures for Major Defense Acquisition Programs ANDATORY (MDAPS) and Major Automated Information Systems (MAIS) acquisition Programs* not only distinguishes Information systems from all other acquisition programs in the title of the document--***THE*** document that directs all DoD agencies on ALL procurement actions, it has a separate chapter devoted to Information Superiority[436] because of its uniqueness. Such a distinction could be interpreted to show that the DoD *is* meeting the challenges of information and a separate service is therefore not required. The document itself belies that interpretation in that its definition of Information Superiority, codified in Chapter 6, "Information Superiority" has a distinctly different definition than does the joint publications it should serve:

> **JP 1-02**: Information Superiority: "That degree of **dominance** in **the information domain** which permits the conduct of operations without effective opposition."[437]
>
> **DoD 5000-2R**: Information Superiority: "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[438]

Further, the DoDI unfortunately does not go far enough, in its definition of a MAIS by excluding highly sensitive classified programs (as determined by the Secretary of Defense) or tactical communication systems. In the latter case, classified systems cannot be optimally used in the combat environment unless they are interoperable, even if compartmented. Overly restricted classification guidelines remains a significant hindrance to acquiring systems. Separate organizations feed this classification problem--a single organization would be instrumental in breaking down unnecessary barriers since it would hold all the security billets. In addition, as new technology becomes outdated, those once highly classified systems will eventually become mainstream and the security would be downgraded. The same standard will greatly ease the transition from black-world to white-world.

Interoperability Critical Performance Parameter (KPP). Further substantiating the uniqueness of IT acquisition programs, note that every major weapon acquisition must have an interoperability common KPP--the only common KPP which pervades every acquisition. Interoperability constraints will form the basis for the CRD and ORD interoperability KPPs.[439]

In addition, the current Air Force acquisition program office is incompatible with the needs of the I-Service. Simply birthing it under the Air Force for example, would only duplicate the flawed structure, used in the Air Force's space and C2 acquisition centers. Both have come under heavy scrutiny by the Secretary of the Air Force who is demanding wholesale restructure of several of the more significant space acquisition programs, including SBIRS.

Any acquisition community in DoD is comprised of several common elements: The Government managers (officers and Government civil service), System Engineering and technical Assistance (SETA) contractors used mainly as technical support and "hands-and-feet", Federally Funded Research and Development Corporations (FFRDCs, e.g. Aerospace Corporation, RAND, Mitre, and CNA), and a contractor base. The traditional contractor base, however, given the significant downsizing the defense industry has undergone since the mid-1980's is ill-prepared to take on this new challenge, as are the FFRDCs. The talent pool lies in industry, whose successes in the area of information dominance eclipsed and surpassed the DoD decades ago. Industry has noted their deficiency and is moving smartly to remain competitive, unlike its military customer. [440] For example, Northrop Grumman (N-G) is attempting to take-over TRW Inc. The take-over "highlights the areas U.S. weapons makers now find important -- space and information, rather than steel and firepower."[441] N-G's strategy is based on filling its gaps in those areas, in that it has the corporate EW and stealth background (N-G builds the B-2 Spirit.) Jeff Bialos, former DUSD for industrial base issues noted "The prime [contractor] of the future is a firm that can integrate onto a platform all the defense electronics and facilitate terrific connectivity between that platform and others in a system-of-systems world."[442]

And although AIS products are procured under different methods, they are still hampered by huge bureaucracies. In addition, the new economy has forced a different issue to the forefront, that of intellectual property. The defense industry has always been concerned with developments of dual-use technology--pouring their own Independent Research and Development (IR&D) moneys into a project only to find the Government refusing to let them reap the benefits.

At the same time, the Government recycles the dogma of the Cold War when defense companies needed to do business with DOD thus putting DOD firmly in the driver's seat. Many government acquisition managers still have that impression. In the traditional acquisition community, particularly the Air Force, the Government is simply incapable of taking a subordinate role. Discussions at the Defense Systems Management College (DSMC) clearly indicated that the military simply does not understand they are no longer in the driver seat on the majority of acquisitions, and take precedence only in very large contracts (like the JSF.) This is a particular problem in the Communications Industry, where the DoD drives only 15% of the requirements, the computer industry, where it drives only 5%, and the software industry, where its influence in negligible. In addition, the traditional defense industrial base is a mere shadow of its former self. It is strong and diversified, but much smaller. Nor do its traditional strengths lie in the IT world. Many of its staunch supporters have in fact migrated to more lucrative markets in keeping with Wall Street priorities--namely the information and communications industries. Nor does the military, the majority of whose officers have not held significant positions in the civilian business world, understand the changing economy in terms of information products. Intellectual property is the lifeblood of many of these companies--shoddy handling in the past by the Government caused significant problems, but could be overcome. Not so in today's information technology. In order to reap the benefits of today's IT, the Government must change its antiquated acquisition strategies.

Chairman Tom Davis, of the Subcommittee on Technology and Procurement Policy, has been raising the issue on Capitol Hill for almost a decade, quoting the *Wall Street Journal* which notes that "three-fourths of the country's top 75 information technology companies will not do research for the Government, citing both difficulty in contracting with the Government and the treatment of intellectual property in R&D contracts."[443] Thus, at the same time that Government is no longer driving technological innovation, many commercial firms that invest billions in R&D every year are refusing to do business with the Government. This has serious implications for the well being of the United States. "Intellectual property rights are the most valued assets of leading-edge technology companies. The Government is challenged today to find ways to entice commercial industry into collaborating with it on vital R&D efforts." [444] This will be difficult given the inherent structure within the DoD and particularly within the acquisition program office. MIT strategist Greg Rafferty agrees and writes:

> "In combination with the pace of change and globalization of information technology activity . . .civilian technological leadership will make government control of the application of new developments with national security implications very difficult."[445]

Carl Builder goes one step further, noting the Constitutional and demographic relationship between the armed forces and society, stating:

> "A nation's military is a reflection and a servant of the society from which it is drawn. If that society undergoes a change as profound as the information revolution, its security requirements will change as well. As a result of these changes, what society asks and expects the military to do to defend the nation, **the military's "enterprise," will almost certainly change**. If so, the most important consequence of the information revolution for the American military will not be the application of new information technologies to its existing missions, as the military perspective often implies. Rather, **the most important** effect will be the need for the military **to adapt itself to performing new and different missions.** The key, then, to understanding how we should apply new information technologies in the military is to [temper the rapid changes and the military utility of those changes.] [emphasis added]."[446]

◆ **<u>The other services are incapable of commanding an Information Service.</u>**

An MNS is not service-specific. Therefore, even though the Air Force is over-tasked (as noted above), the other services may be able to take on the mew mission area, and thus obviate the need for a new service. Research, however, indicates they too are overwhelmed. The Army is in the midst of a massive transformation into a lighter, leaner force and lacks an extensive experience base in space and EW. The Navy, however, has extensive experience in space. Unfortunately, they have been highly criticized by Congress on their transformation efforts. Ronald O'Rourke, an analyst with the Congressional Research Service who

> "wields unusual influence on Capitol Hill, where Republican and Democratic lawmakers alike frequently cite his reports on weapons programs and call him as an expert witness when conducting their annual budget hearings, [notes] Unlike the U.S. Army and Air Force, the **Navy does not have a clear, concise plan for transformation** that can quickly explain to defense decision-makers what the maritime service is doing to **make itself relevant in the 21st century**." [Most troubling was O'Rourke's assessment that] "[t]here are plenty of transformation efforts in the Navy, but there **is no single, overarching framework** [emphasis added.]"[447]

This is particularly critical given that the single most important element of information operations is *a priori* architecting. Other independent analysts echoed O'Rourke's assessment of the Navy's posture on military reform.[448] These deficiencies would spill over to Congressional support. Most importantly, the current military structure is simply incapable of the enormous task that lies ahead, and the requisite structure this I-Service would entail.

<u>OS1: The QDR calls for significant transformation</u>. The QDR explicitly recognized the need to radically transform the Armed Forces, devoting an entire chapter to eliminating redundancy, revising organizational structure, and taking judicious risks in experimenting with new organizational design. Previous transformations were undertaken to improve, streamline and save costs.

Secretary Rumsfeld instead believes transformation is critical to the nation's **vital interests**. In the QDR, he states:

> "Achieving the objectives of the defense strategy requires the transformation of the U.S. Armed Forces. Transformation results from the exploitation of new approaches to operational concepts and capabilities, the use of old and new technologies, and new forms of organization that more effectively anticipate new or still emerging strategic and operational challenges and opportunities and that render previous methods of conducting war obsolete or subordinate. . . .Transformation is at the heart of this new [capabilities-based] approach. The Department's leadership recognizes that continuing "business as usual" within the Department is not a viable option given the new strategic era and the internal and external challenges facing the U.S. military. **Without transformation, the U.S. military will not be prepared to meet emerging challenges**."[449]

The QDR further recognizes the RMA. "The ongoing revolution in military affairs could change the conduct of military operations. Exploiting the revolution in military affairs requires not only technological innovation but also development of operational concepts, **undertaking organizational adaptations**, and training and **experimentation to transform a country's military forces**."[450]

One must not transform for transformation's sake. Transformation must be necessary, measured, and tempered, and "focused on emerging strategic and operational challenges."[451] The QDR further notes that

> "it would be imprudent to transform the entire force all at once. A balance must be struck between the need to meet current threats while transforming the force over time. DoD will explore additional opportunities to restructure and reorganize the Armed Forces."[452]

The transformation to an I-Service meets these criteria and are specifically linked to both the majority of Transformation goals, and all four transformation pillars. The goals are as follows:

- "Assuring information systems . . . and conducting effective information operations;
- Denying enemies sanctuary by providing persistent surveillance, tracking

- Enhancing the capability and survivability of space systems and supporting infrastructure;
- Leveraging information technology and innovative concepts to develop an interoperable, joint C4ISR architecture and capability that includes a tailorable joint operational picture."[453]

The pillars are as follows:

- ". . .Improved joint command and control . . .
- Experimenting with new approaches to warfare, operational concepts and capabilities, and organizational constructs . . .
- Exploiting U.S. intelligence advantages through multiple intelligence collection assets, global surveillance and reconnaissance, and enhanced exploitation and dissemination;
- Developing transformational capabilities through increased and wide-ranging science and technology, selective increases in procurement, and innovations in DoD processes."[454]

The QDR goes on to direct significant changes in the DoD, its Services, and the Defense Agencies, noting, "[t]he [DoD] must also align, consolidate, or differentiate overlapping functions of the U.S. Government Printing Office, the Services, and the Joint Staff. To do this, DoD will develop recommendations to eliminate redundancy. In addition, the DoD will require transformation roadmaps for Defense Agencies to seek efficiencies."[455]

OS2: IO may require new LOAC. Information Operations clearly does not fit within the scope of existing Laws of Armed Conflict (LOAC) as well. Any citizen can attack elements of a nation's infrastructure (even that of its own sovereign) from a home computer. This creates a conundrum when trying to define the term "legal combatant." Hundreds of Chinese students attacked the US's computer infrastructure after the accidental bombing of the Chinese embassy--the US of course did not retaliate against China. Similarly, the world grappled with the concept of massive civilian morale bombings in the early 1920's, even as the Hague implicitly outlawed the action against the civilian morale bombing campaigns so forcefully espoused by Douhet. **It took the creation of a**

separate service to corral this new weapon. Similarly outcries were heard when the concept of space weaponization became possible--the world demanded international bans on this new weapon. No new service was created however, instead this new element adopted its progenitor's conscripts with little thought. They are only now being revisited-40 years after conception, and DoD's critical space assets remain vulnerable in part due to the conundrum posed. Information Operations is experiencing a similar trend--these systems can be, and have proven to be, so very ruinous, international law is being hotly debated. A definition will provide the starting point, because it's needed to define the doctrine, and that doctrine will only be developed once a single lead is determined. Only then can international law determine its eventual evolution.

That the Air Force is tied to prevailing conscripts of kinetic weapons is not pejorative. Even lawyers return to the definition of kinetic effects when trying to ascertain the effect of an information attack. Generally speaking, according to Col Dunlap citing UN Charter 51:

> "Clearly, [IO concepts] …are largely predicated on the assumption that "armed attacks" and similar provocations will employ kinetic weapons. The legal situation is less clear when the "attack" occurs digitally and consists merely of the manipulation of data. . . . An "armed attack" for the purposes of Article 51 is considered to have occurred when the characteristics and effects of the cyber-strike equate to those that result from a traditional kinetic weapon attack."[456]

DoD's Office of General Counsel, in their report "An Assessment of International Legal Issues in Information Operations," completed in May 1999 after Deliberate Force raised troubling concerns, dedicated an entire chapter to International Efforts to Restrict

Information Operations. In fact,

> "the first public governmental initiative was a resolution tabled by Russia in the UN's First Committee in October 1998 that apparently reflected a serious effort to get the UN to focus on the subject. The Russian resolution included a call for states to report their views regarding the advisability of elaborating international legal regimes to ban the development, production and use of particularly dangerous information weapons." The United States feels such debate at this times is premature.[457]

This position is troublesome. The US is appropriately concerned about an imminent space war, but such a war requires significantly more sophisticated means than does an IO attack (as noted in Chapter 2)--it is far more difficult to jam a satellite link than it is to disable an information infrastructure--**which carries the product of that satellite link**. The US is too narrowly focused on the source rather than the system--it's all information and that information must be protected from end to end.

The report also notes: "There is no legal prohibition against developing and using space control weapons, whether they would be employed in orbit, from an aircraft in flight, or from the Earth's surface [with the notable exception of nuclear weapons]."[458]. The issue is confusing, but the law is clear: **there are no laws banning space weapons**. There *are* four applicable treaties that govern space weapons, whose precepts can be summarized as follows:

- Sovereignty: No nation can claim space for sovereign use and thus space "is free for exploration and use by all nations."[459]
- "Golden Rule": "Activities in space shall be conducted with due regard for the interests of other states." [460]
- Liability: :States that launch space objects are liable for any damage they may do in space in the air, or on the surface of the Earth." [461]
- General: Space activities are subject to general principles of international law, including the UN Charter.

In essence, these laws outline permissable and non-permissable actions:

Permissable:

- Space-based weapons including OCS and DCS weapons

Non Permissable:

- Nuclear testing in Outer Space (including using a nuclear device as EMP weapon)
- Space-based TMD systems, a treaty the US is unilaterally withdrawing from and which the Senate never confirmed
- Any action that would impact national technical means for treaty verification

But again, clear standards on what is "use of force" are not clear, and without clear intelligence, interference cannot be ascertained. The level of conflict must also be established to determine rights with respect to active defense and offensive action. Legally,

> "If the principle of noninterference is regarded as suspended for the period of the conflict, it also seems likely that the liability provisions in these agreements would also be suspended, at least between the parties. This would not, however, excuse the belligerents from liability to neutral nations if their actions caused damage to their citizens or property." [462]

This is a particular concern given the use of consortium constellations and the fragility and temporal nature of the data they carry. In essence, the report clearly indicated the synergy between the laws of traditional space control and the laws governing information operations. **In addition, it clearly sets new precedents in interpretation of the Geneva and Hague Conventions.** In fact, even US Domestic Law and Policy seem harsher, in that *it is a felony* to intentionally or maliciously interfere with a communications or weather satellite, or to obstruct or hinder any satellite transmission."[463]

In terms of communications law, "International communications law contains no direct and specific prohibition against the conduct of information operations by military forces, even in peacetime."[464] There are a number of treaties, however to prevent intentional interference with communications of other members. This includes all aspects of space control negation precepts: Deny, Deceive, Disrupt, Degrade, or Destroy. In fact, Articles 19 and 20 of the Nairobi Convention specifically "allows members to "stop the transmission of any private telegram which may appear dangerous to the security of the State or contrary to their laws [and to generally] suspend the international telecommunication service for an indefinite time upon immediate notification of the aggressor."[465]

Col Dunlap, in *Cyberwar 3.0* notes with respect to IO that one must be "conscious of what the law does or does not permit if, for no other reason than the failure to be sensitive to these concerns, may well lead to operational failure." He argues that there does exist a body of law despite the rhetoric, but that "it may be that there are certain areas where the law needs development or clarification . . . given the issue's complexity." [466] Therefore IO confuses such issues as the Geneva Convention, the Hague Convention, LOAC, and even calls into question concerns with *jus ad bellum* and *jus in bello*. [467]

Col Dunlap has a different perspective of defining acts of war with respect to IO, returning to the legal perspective, and noting

> "there are only two bases to use armed force subsequent to the ratification of the UN Charter that, in essence, outlawed war. The two situations still authorizing the use of armed force are: 1) pursuant to a UN Security Council Resolution 2) in self-defense in response to an "armed attack" pursuant to Article 51 of the Charter."[468]

He likewise noted that all attacks must comply with principles of war, including discrimination and proportionality.[469]

An I-Service meets analogous tenants of Information Power as Mahan described for Seapower.

Table 25 further establishes the I-Service meets the tenets of an Information-faring nation, in the same fashion as did Sir Alfred Mahan[470] for a sea-faring nation, proving that Information Power is just as critical as naval power given the extent the national economic and social fabrics are tied to information. Yet unlike Seapower, Information has no consolidated power base despite marked vulnerabilities.

Table 26: Information Service in the Tradition of Mahan

Condition[471]	Interpretation ITO Seapower	Seapower Condition Met?	Interpretation ITO Information Power	Information Power Condition Met?
Geographical position	- Geostrategic location of the nation - Extent of isolation from other countries by oceans -Extent nation is protected through geography	- Yes--United States is geostrategically located - Protected being isolated in this hemisphere - Deftly acquired territory[472] to ensure access to sea routes	- Extent nation is integrated with the *international* information infrastructure	- Yes--Extensively interconnected with World Wide Web, the Internet, phone system, SatCom, multimedia, etc.
Physical conformation	- Typography of the nation's coastline, littoral regions	- Yes--Extensive--coastline is impenetrable in many areas - Have extensive, mature ports throughout coast - Have extensive inland waterways	- Extent of interstate information technology	- Yes--Extensive--US has most extensive communications infrastructure, web connections, and "electronic" web connecting its "industrial web"
Extent of territory	- Circumference (length) of the coastline	- Yes--Extensive--too large to be breached entotale	- Pervasiveness of information technology throughout the nation	- Yes--Extensive--commerce, military, educational institutions, society pervaded
Number of population	- Number of the population	286.6M in US vs. 6.2B[473] in the world. Thus while US comprises only < 5%, it has the largest GDP and is the only remaining superpower	- Number of the population	286.6M in US vs. 6.2B474 in the world. Thus while US comprises only < 5%, it has the largest GDP and is the only remaining superpower

Table 25 (Cont.): Information Service in the Tradition of Mahan

Condition[475]	Interpretation ITO Seapower	Seapower Condition Met?	Interpretation ITO Information Power	Information Power Condition Met?
National character	- The extent the nation is a "seafaring nation" Extent the country is dependent on, and embraces the sea to perpetuate its IOPs	- Yes--Military: USN receives majority of DoD funding and crucial to power projection and Global reach - Economy wholly dependent on access to sea - Politically: Deterrent threat of USN - Carriers are perfect "floating ambassadors" and are US sovereign territory	- Extent the nation's populace is dependent on IT for its IOPs and is technologically orientated	- Yes--Military: Critically dependent on C4ISR architecture and information but unprotected at this time - Economy wholly dependent on IT--banking system, power grid, communications infrastructure, etc. - Politically: Communications - Deterrent threat of DoD - Socially: US is the most wired country in the world and dominates software and advanced computer chip manufacturability
Character and policy of governments	- Extent the Government supports Seapower - Extent Government policies support technology - Extent of the history of the nation wrt Seapower	- Yes--USN receives majority of DoD funding--has littoral forces, commercial protraction (USCG) and Merchant Marine - Nation's emergence as world power tied inextricably to Seapower	- Extent Government supports information technology - Extent Government policies support technology - Extent of the history of the nation on IT	- Yes--Government fully supports IT - Government has been inconsistent in its policies on IT - US invented computer, internet, e-commerce, and has the most extensive IT-based economy, C4ISR architecture and space assets than any country - Technology has always been a unique element of the American Way of War

Notes

[341] Maj Shawn P. Rife, "On Space Power Separatism." In *Airpower Studies: AP Coursebook Academic Year 2002*. Compiled by LtCol Micheal Fiedler, Phd, et al. Air

Notes

Command and Staff College: Department of International Security and Military Studies. Maxwell, AFB, AL. Aug 2001, 393.

[342] Ibid.

[343] Robert Wall. "Costs Cast Shadow On F-22 Go-Ahead." Aviation Week & Space Technology, 3 August 2001, n.p.

[344] Ibid.

[345] The Air Force believes it will be only $2 billion over the limit, with savings measures planned. Which of the two estimates is more accurate is unclear, says the General Accounting Office's (GAO's) Allen Li, although he told lawmakers last week that in the past the more conservative estimates have proven more accurate.

[346] Wall, "Costs Cast Shadow On F-22 Go-Ahead."

[347] Wall, "Costs Cast Shadow On F-22 Go-Ahead."

[348] "F-22 Headed for Reprieve From Congressional Ax." *Aviation Week & Space Technology*, 9 August 1999, 28-29.

[349] Thompson, Dr. Loren B. "US Must Reverse Bomber Blueprint, Air Force Dominated by tactical fighter community, experts say." National Defense. July/Aug 1999. On-Line. Internet, Available from http://www.lexingtoninstitute.org/defense/revbmb.htm.

[350] Ibid.

[351] Ibid.

[352] Ibid.

[353] Ibid.

[354] Ibid.

[355] Ibid.

[356] Ibid.

[357] Vago Muradian. "Air Force Considers Speeding Up C-130J Buy to Control F-22 Cost." Defense Daily, 23 Oct 99, n.p. On-line. Internet, 2 January 2002. Available from www.d-n-i.net/FCS_Folder.

[358] Mark Selinger. "Senate Panel OK's USAF's 767 Lease Plan." Aviation Week & Space Technology, 5 Dec 01, n.p. On-line. Internet, 1 Jan 2002. Available from http://www.aviationnow.com/avnow/news/channel_military.jsp?view=story&id=news/m7671205.xml

[359] George Cahlink. "Replacing an Aging Fleet." Government Executive, 1 August 2001. GovExec.com. On-line. Internet, 1 August 2001, n.p. Available from http://www.govexec.com/top200/01top/s7.htm

[360] Statement of Congressman Pitts, Joseph R. "Surveillance and Support: Shortfalls in Electronic Warfare, 9 Sep 99.

[361] Representative Joseph R. Pitts. "Electronic-Warfare Assets Badly Neglected." *National Defense*, June 2000, 39.

[362] Ibid.

[363] Loren B. Thompson, PhD. "The Future of Airborne Electronic Warfare." Lexington Institute. Available ON-line Internet. http://www.navyleague.org

[364] Statement of Congressman Pitts.

[365] Ibid.

Notes

[366] Today, there are 124 EA-6B Prowlers organized in 19 squadrons-10 carrier-based, eight expeditionary (land-based) and one reserve." (See: Pitts, Representative Joseph R. "Electronic-Warfare Assets Badly Neglected." National Defense, June 2000, 39.)

[367] Thompson, "The Future of Airborne Electronic Warfare

[368] Pitts, "Electronic-Warfare Assets Badly Neglected," 40.

[369]Ibid.

[370] Ibid.

[371] Ibid.

[372] Ibid.

[373] Maj Jeffery T. Butler. *UAVs and ISR Sensor Technology*. Maxwell AFB, AL: Air Command and Staff College, Apr 2001, 1

[374] QDR, 47.

[375] David A Fulghum. "Pentagon Champions UAVs, Communications." *Aviation Week and Space Technology*, 17 Dec 2001, n.p. On-line. Internet, 3 February 2001. Available from http://www.aviationnow.com/content/publication/awst/20011217/avi_news.htm.

[376] Butler, 6.

[377] Ibid.

[378] Ibid..

[379] Ibid.

[380] David A. Fulghum and Wall, Robert. "Global Hawk, J-STARS, Head for Afghanistan." *Aviation Week and Space Technology*, 5 Nov 2001.

[381] Department of Defense. *Quadrennial Defense Review Report*. Washington DC: U.S. Government Printing Office, Sep 2001, 52.

[382] Bruce Rolfsen. "On-the-job-testing." *Air Force Times*. 21 Jan 2002, 12-13.

[383] Ibid.

[384] David A. Fulghum. "Stealthy UAVs Snag Rumsfeld's Attention." *Aviation Week and Space Technology* 4 Jun 01.

[385] Department of Defense. *Quadrennial Defense Review Report*. Washington DC: U.S. Government Printing Office, Sep 2001, 49. (Note: Based on increase from current R&D funding levels of 2%, increased to 3%.)

[386] Fulghum, "Stealthy UAVs Snag Rumsfeld's Attention."

[387] Ibid.

[388] Ibid.

389 Ibid.

390 Ibid.

[391] Capt David A. Turner. "Bullet Background Paper On UAV Comm Issues." Bullet Background Paper, AC2ISRC, 30 Mar 00.

[392] Ibid.

[393] Rolfsen, 12-13.

[394] Ibid.

[395] The JDAM is not a bomb itself, but kit made by Boeing that fits onto traditional gravity,, or dumb bombs, turning each into a PGM.

Notes

[396] Homeostatic RADAR (Radio Detection and Ranging) sends out a signal and receives the echo of that signal using physics (differential speed) to determine range, and Doppler to determine range rate. Bi-static radar uses separate transmitters and receivers. Multiple receivers can be then be linked by a communications net.

[397] Bill Sweetman. "Stealth Threat." *Popular Science*. Dec 2001, n.p. On-line. Internet, 8 Feb 2002. Available from http://www.popsci.com/popsci/aviation/article/0,12543,188700-1,00.html.

[398] Scott Canon. "Stealth Unmasking Only a Matter of Time." 17 Jun 2001. Kansas City Star.

[399] Sweetman, "Stealth Threat."

[400] When a cellphone tower sends out a signal, each receiver hears it twice. The first signal comes directly from the tower and the second is an echo from the target. If three or more receivers measure the time difference between the two signals, using GPS to provide precise synchronization of the arrival times, they should be able to pinpoint the target.

[401] Jason Bates. "Software Could Lead to Low-Cost Supercomputer." *Space News*, 21 January 2002, 4.

[402] Sweetman, "Stealth Threat."

[403] Work is progressing on stealth- improving methods that have nothing to do with a plane's shape. Edges and other "hot spots" on stealth aircraft can be treated with plastics or paints that contain radar-absorbing inks, powders, or mineral compounds. Notably, those materials are most effective in the microwave band where cellphones operate.

[404]"Early on, engineers tried to camouflage airplanes using special paints and coatings. It didn't work. In 1958, the CIA sent a camouflaged U-2 on a spy flight across Russia. Attached to the subsequent protest note from Moscow was a detailed radar plot of the airplane's flight path."

[405] "The F-117 and B-2 also have long, straight edges that focus radar reflections into single, concentrated beams. The way the plane's edges are angled, the beams shoot off to the side, rather than directly back at the antenna that sent the signal. "

[406] Sweetman, "Stealth Threat."

[407] Ibid.

[408] Ibid.

[409] Fulghum, "Stealthy UAVs Snag Rumsfeld's Attention."

[410] Keith R. Hall. "Space Policy, Programs, and Operations." Presentation to the Committee on Armed Services: Subcommittee on Strategic forces," 8 Mar 2000. On-line. Internet, 22 December 2001.Available from http://www.senate.gov/~armed_services/statemnt/2000/000308kh.pdf.

[411] Gen. Richard B. Meyers. "Commander In Chief, U.S. Space Command Testimony Before the U.S. Senate Strategic Forces Subcommittee Senate Armed Services Committee. 22 Mar 1999, n.p..

[412] Ricky B. Kelly. "Centralized Control of Space: The Use of Space Forces by a Joint Force Commander." School of Advanced Airpower Studies. Air University Press. Maxwell Air Force Base, Alabama. 28 June 93, 21.

[413] This figure is also supported by Rattray, 39

Notes

[414] CDR Andy Wilde. “Update: Information Operations: A common Perspective.” *USACOM Joint Warfighting Center’s Newsletter 6*, No. 2 (October 1998): 8.

[415] Linda de France. “Ryan Says Space Force Unwarranted For Next 50 Years.” *Aerospace Daily,* 9 Feb 01, n.p. .On-line. Internet, 18 Jan 2002. Available from http://home.datawest.net/dawog/Space/e20010209space_force_unwarranted.htm.

[416] “The Inflation Calculator.” On-line. Internet, 2 Jan 2002, n.p. Available from http://www.westegg.com/inflation/infl.cgi.

[417] Ibid.

[418] Alton Frye. “Our Gamble in Space: The Military Danger.” The Atlantic Monthly, August 1963, n.p. On-line. Internet, 12 Oct 2002. Available from http://www.theatlantic.com/issues/63aug/frye.htm

[419] QDR, 53.

[420] Encyclopedia Astronautica. Available On-line from: http://www.friends-partners.ru/partners/mwade/chrono/19723.htm

[421] James M. Smith. USAF Culture and Cohesion: Building and Air and Space Force for a 21st Century. Institute for National Strategic Studies. Occasional Paper 19. Colorado Springs, CO: USAF Institute for National Security Studies, June 1998, 6.

[422] Smith, USAF Culture and Cohesion, 6.

[423] Ibid.

[424] Ibid.

[425] Ibid.

[426] Ibid.

[427] Kanter does not address the Marine Corps, but it has all of the cohesive elements found with the Army plus the additional advantages of a narrow mission set and a small size. The Marines are organized into an organic whole, the Marine Air-Ground Task Force.

[428] Kanter does not address the Marine Corps, but it has all of the cohesive elements found with the Army plus the additional advantages of a narrow mission set and a small size. The Marines are organized into an organic whole, the Marine Air-Ground Task Force.

[429] Smith, “USAF Culture and Cohesion,” 6.

[430] Toby Harnden. “Rumsfeld Calls For End To Old Tactics Of War.” *London Daily Telegraph*, 16 October 2001.

[431] AP class notes, May 2001.

[432] John A. Tirpak. “The New World of Information Warfare.” Air Force Magazine, 1996. On-line. Internet, 20 Dec 2001. Available from http://www.afa.org/magazine/toc/06cont96.html, n.p.

[433] LtCol Anthony Christopher Cain. “Neither Decadent, nor Traitorous, Nor Stupid: The French Air Force and Doctrine in the 1930s.” Ph.D. Thesis, Ohio State University, 2000.

[434] An AIS that is designated by ASD(C3I) as a MAIS, or estimated to require program costs in any single year in excess of $32 million in fiscal year (FY) 2000 constant dollars, total program costs in excess of $126 million in FY 2000 constant dollars, or total life-cycle costs in excess of $378 million in FY 2000 constant dollars.

Notes

[435] dodi_5000_2_final_version_jan_04_2001

[436] The acquisition guidelines direct the services to "attain information superiority through the acquisition of systems and families-of-systems that are secure, reliable, interoperable, and able to communicate across a universal IT infrastructure, to include NSS. This IT infrastructure includes the data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities.

[437] JP 1-02

[438] 5000-2R DoD 5000-2R, "MANDATORY PROCEDURES FOR MAJOR DEFENSE ACQUISITION PROGRAMS (MDAPS) AND MAJOR AUTOMATED INFORMATION SYSTEM (MAIS) ACQUISITION PROGRAMS. 10 Jun 2001.

[439] For the acquisition community, the interoperability requirements established in the requirements process shall be allocated from the requirements documents to the individual systems through the system engineering process.

[440] Greg Schneider. "Contractors Target New Technologies -- And Each Other." Washington Post. 23 February 23, 2002, n.p

441 Ibid.

442 "Contractors think they will be better able to provide that future if they control broad areas of military technology: a Northrop Grumman-built Global Hawk spy drone can talk to a Northrop Grumman satellite and relay information to a Northrop Grumman command system on a destroyer. Such thinking made the move to buy TRW "classic Northrop Grumman: aggressive and opportunistic and smart." (See:: "Contractors Target New Technologies -- And Each Other." *Washington Post.* 23 February 23, 2002, n.p)

[443] US House. *HEARING NOTICE: Transforming the IT and Acquisition Workforces: Using Market-Based Pay, Recruiting and Retention Strategies to Make the Federal Government an Employer of Choice for IT and Acquisition Employees.* 101st Congress, Subcommittee on Technology and Procurement Policy, 2 Oct 01. n.p.

[444] Ibid.

[445] Gregory J Rattray. *Strategic Warfare in Cyberspace.* The MIT Press. Cambridge, MA. P. 66

[446] Zalmay M. Khalilzad and John P. White. *Strategic Appraisal: The Changing Role of Information In Warfare*. Santa Monica, CA: RAND Corporation, 1999, 19.

[447] Tom Canahuate. "Analyst Says U.S. Navy Lacks Unifying Transformation Plan." *DefenseNews.com* 16 Jan 2002.On-line. Internet, 18 Jan 2002. Available from http://www.defensenews.com.

[448] Dale Eisman. "Navy Criticized For Failing To Reshape Its Role. Norfolk Virginian-Pilot. 17 Jan 2002, n.p.

[449] QDR, 24.

[450] Ibid, 14.

[451] Ibid, 38.

[452] Ibid, 31.

[453] Ibid, 38.

[454] Ibid, 40.

[455] Ibid, 62.

Notes

[456] Capmden, 138

[457] Department of Defense Office of General Counsel. *An Assessment of International Legal Issues in Information Operations*. Washington D.C.: US Government Printing Office, May 1999, 52.

[458] Ibid, 35.

[459] Ibid, 31.

[460] Ibid.

[461] Ibid.

[462] Ibid, 32.

[463] Ibid, 29.

[464] Ibid, 38.

[465] Ibid, 37.

[466] Campden, 140-1.

[467] Ibid.

[468] Ibid.

[469] Ibid.

[470] Sir Alfred Mahan put forth six principles to determine the extent a nation could be considered a Seapower, and the extent to which it could depend on that Seapower in times of crisis. He used these six principles, "universal and timeless in character" as a means to support the continued growth of naval Seapower, an approach enthusiastically embraced by the British (who knighted him for his vision) and successfully used by US sea power advocates.

[471] Sir Alfred Thayer Mahan. "Excerpts from: The Influence of Seapower on World History." From *The Influence of Seapower Upon History: 1660-1783*, published by Dover Publications, Inc., New York, 1987. In Air Command and Staff College Distance Learning Program. Lesson TH506r01. CD-ROM ACSC Multimedia Edited Version 2.2., Aug 1997, n.p.

[472] Dr. J. T. LaSaine, Jr. "The Realist Tradition in the United States Foreign Policy." Lecture. Dept of International Security and Military Studies. Air Command and Staff College. Maxwell AFB, AL, 27 Aug 01.

[473] As of 4 Mar 2002, actual numbers are estimated to be 286,561,349 for US and 6,209,365,430 in the world. (See: "U.S. Census Bureau Homepage." US Department of Commerce, 4 Mar 2002. On-line. Internet, 4 Mar 2002. Available from http://www.census.gov/.

474 As of 4 Mar 2002, actual numbers are estimated to be 286,561,349 for US and 6,209,365,430 in the world. (See: "U.S. Census Bureau Homepage." US Department of Commerce, 4 Mar 2002. On-line. Internet, 4 Mar 2002. Available from http://www.census.gov/.

[475] Mahan.

Appendix E

Details of Chapter 5: The Information Service

> *The need to transform America's military capability encompasses more than strategy and force structure. Transformation applies not just to what DoD does, but how DoD does it. During the same period that the security environment shifted from a Cold War structure to one of many and varied threats, the capabilities and productivity of modern businesses changed fundamentally. The Department of Defense has not kept pace with the changing business environment. While America's business have streamlined and adopted new business models to react to fast-moving changes in markets and technologies, the Defense Department has lagged behind without an overarching strategy to improve its business practices.*
>
> —2001 Quadrennial Defense Review

> *The Department must also align, consolidate, or differentiate overlapping functions of the Office of the Secretary of Defense, the Services, and the Joint Staff. To do this, DoD will develop recommendations to eliminate redundancy.*
>
> —2001 Quadrennial Defense Review

Section IV of a Mission Needs Statement[476] analyzes a *materiel* solution--i.e. it addresses current systems that could counter the threat identified earlier. That materiel solution must comply with national policy as promulgated in the NSS, QDR and JV2020. In terms of I-Service, Chapter 2 described the threat as broad an enduring, Chapter 3 discussed the need, and Chapter 4 proved a non-materiel solution was required. This appendix provides a strawman concept on a potential materiel solution. As such, it too must comply with national strategic direction.

This chapter now focuses on the essential elements that would comprise that service, whether independent or not, explaining the necessary calculus of its military, civilian, and industrial components, based on the analysis completed in Chapter 4--namely, the incompatibility of the current program office construct, unique IT acquisition policies, the need to focus limited resources, and the QDR's demand for consolidation. The resultant calculus must embody some of the key tenets proven--namely integration and the need for a core industrial base supporting a military structure that can both fulfill its Title 10 requirements for a Service, as well as OPCON its combatant forces to a combatant command. Using existing constructs, e.g. Title 10, Posse Comitatus, personnel resources, industrial base, and current government organizations, the function would:

1. Need to fulfill its Title 10 obligations in the lawful conduct of offensive action
2. Have a similar structure to that of the Coast Guard to optimize the civilian-military duality of its mission while not violating Posse Comitatus
3. Consist of minimal government (both military and civil service) performing only Inherent Government Functions
4. Have a significant industrial component and augmented industrial base
5. Develop a single acquisition center for C4ISR, space information systems, and intelligence products

1. Fulfill its Title 10 obligations. The I-Service must have a small, elite force that can "pull the trigger" when its forces are OPCON'd to a Joint Force Commander:

> . ". . .[S]oldiers are trained when to use or not to use . . .force. Escalation is the rule. The military exists to carry out the external mission of defending the nation. Thus, in an encounter with a person identified with the enemy, soldiers need not be cognizant of individual rights, and the use of deadly force is authorized without any aggressive or bad act by that person."[477]

Government civilians, except through Presidential directive (e.g. CIA actions), cannot take up offensive arms against a nation as a legal combatant--nor can contractors. And nor *would* contractors--these industries are part of a large multinational construct in a highly competitive industry--information and space. They cannot risk market capitol of executing actions which could disable the very systems they are trying to sell on the international market. Nor could the Government entrust such responsibility to an industry that may refuse to act given its foreign customers and/or ownership, or which becomes a terrorist target as a result of supporting the American Military Machine. The impact of a Boeing, for example, trying to sell satellites while also working on space control systems to negate those satellite services would be a significant detractor with respect to the international community, and only serve to weaken the US's already diminishing role in space commerce, promulgated by the unnecessary restriction on exporting satellite technology which has negatively impacted it.[478]

This is not mere speculation. Given *EutelSat*'s contractual commitments to Yugoslavia, it took diplomats several weeks to convince the EutelSat consortium to default on its SATCOM communications contract with Yugoslavia to stop its propaganda-fueled-SATCOM-delivered cleansing of ethnic Kosovors. Likewise, "shutter control" against space systems may not always work, even if the DoD continues to pay handsomely to monopolize service due to perceived future profits, the very growth of the market, external threats, or a foreign-owned company's own national interests.

James Adams, author of the Next World War, explained it best:

> "We need a deterrent strategy for cyberspace just like we have for nuclear war or conventional war," he said. "The Department of Defense has to step up to the plate because they have the capability and the responsibility."[479]

2. Have a similar structure to that of the Coast Guard to optimize the civilian-military duality of its mission while not violating Posse Comitatus. Posse Comitatus, a law dating back 120 years, despite its antiquated structure, is essential to ensuring the armed forces remain firmly under civilian control and are never used against the civilian populace, except in those extreme cases identified by the President. "The Act embodies the traditional American principle of separating civilian and military authority and currently forbids the use of the Army and Air Force to enforce civilian laws."[480] However, exceptions have been granted and are being granted on an increasing basis. The exceptions include aiding drug-trafficking (which later expanded into the armed forces becoming "single lead agency" in drug interdiction efforts), and in domestic problems including the bombing of the Muir building, as well as in matters of intelligence with respect to the United States Coast Guard (USCG).[481]

The legal structure of the Coast Guard regarding its employment, in fact, provides an appropriate precedent, one the I-Service would duplicate, in that it, like the USCG, would be firmly rooted in both the civilian and military realms. The Coast Guard is specifically waived from Posse Comitatus[482] in Title 10 due to its multi-function roles. (It is interesting to note the analogy to the birth of the Coast Guard as well with respect to the I-Service--both were developed to protects "ports of entry" the former physical, the latter electronic.)[483] The US Coast Guard is a military service, and falls under the Department of Transportation during peacetime, and under the Naval Department in wartime only when "chopped" to the USN "upon declaration of war or when the President directs."[484] The Coast Guard likewise operates in a complex and dangerous maritime environment characterized by rapidly changing security threats at home and abroad. There is no better, no more fitting, precedent for the I-Service. Thus, the I-Service would be considered a military service, but not be shackled by Posse Comitatus when executing its necessary duties.

3. Consist of minimal government (both military and civil service) performing

only Inherent Government Functions. Because industry forms such a significant core, and in line with the MNS construct, the traditional structure of the acquisition community must also be addressed. The following elements are considered in order: inherent government functions, Government personnel, and Government technical advisors.

Inherent government functions. Policy Letter, 92-1 "Inherent Government functions," describes those functions that must be executed by a Government employee. An inherently governmental function (IGF) is a function that

"is so intimately related to the public interest as to mandate performance by Government employees. These functions include those activities that require either exercise of discretion in applying Government authority or to the making of value judgments in making decisions for the Government."[485]

Government functions normally fall into two categories:

1. the act of governing, i.e. the discretionary exercise of Governmental authority, and
2. monetary transactions and authority

As it is currently interpreted, almost all program office functions, excluding those directly related to command, contracting, and fiscal matters, could be executed by industry, resulting in more responsibility *appropriately* transferred to industry. After almost ten years of consistently narrowing the IGF definition, where more functions are recognized as being appropriate for outsourcing to industry, 92-1 is under extensive revision and promises more opportunities for outsourcing. The *Union* states:

> ". . . it appears as if the New Administration will be striving to improve the efficiency of Defense operations through competitive sourcing and privatization" and that" the public can reasonably expect an increase in the number of functions outsourced."[486]

In addition, the QDR demands the DoD:

> Focus DoD-owned resources on excellence in those areas that contribute directly to warfighting. Only those functions that must be performed by DoD should be kept by DoD. Any function that can be provided by the private sector is not a core government function. Traditionally, "core" has been very loosely and imprecisely defined and too often used as a way of protecting existing arrangements."[487]

The QDR divided these functions into three broad categories:

> 1. "Functions directly linked to warfighting and best performed by the federal government. In these areas, DoD will invest in process and technology to improve performance"[488]
>
> 2. "Functions indirectly linked to warfighting capability that must be shared by the public and private sectors. In these areas, DoD will seek to define new models of public-private partnerships to improve performance." [489]
>
> 3. "Functions not linked to warfighting and best performed by the private sector. In these areas, DoD will seek to privatize or outsource entire functions or define new mechanisms for partnerships with private firms or other public agencies."[490]

This direction embraces outsourcing more and more responsibility to industry. Likewise, it will infuse additional capitol into the information industry which will pay dividends in terms of the other Instruments of Power, particularly in the economy. This is supported by Michael Assante, VP of intelligence at Vigliniex, a provider of managed security products and service who noted his larger concern "with the private sector's stability to deal with [cyberattacks] . . .private companies don't have the resources the government has in order to protect themselves."[491] It's a two way street--the DOD would benefit from increased collaboration at the same industry would benefit from increased investment and increased insight. This is critical to the overall health of the national infrastructure and directly support the military IOP as noted in the following passage from a RAND study:

> "Because the United States and its democratic partners are **more economically dependent** than other countries on connectivity and computing, they can become **more vulnerable to information warfare**, even ending sanctuary from hostile attack that they now enjoy. Integration in world economy, with its crisscrossing networks, enlarges the risk. Threats to the democracies' cyberspace endanger **not only the citizens' quality of life but also their resolve**. Americans are ambivalent enough about projecting power as it is. The prospect of a disruption of the national economy due to attacks on domestic information infrastructure could tilt that ambivalence in a distinctly negative direction, **thus emboldening a militarily inferior enemy to challenging U.S. interests**. Moreover, as the United States and other advanced nations more dependent on information technology in their military systems, they will become more susceptible to information warfare in operations. The revolution in military affairs places a bull's eye on the C4ISR that is critical to it. In the extreme, the ability of United States to project power and to strike at will could be undermined if an otherwise weaker enemy interfered with the links that network U.S. forces, fuse U.S. sensor data, and permit joint warfare. **Even if the military establishment secures its own dedicated links and nodes, effective information warfare attacks on the U.S. public telecommunications network, on which nearly all routine military traffic flows, could create havoc in a crisis and cripple a major power-projection campaign**[emphasis added.][492]

<u>Government Personnel.</u> The government does not have the military or civilian capitol to execute the whole of Information Operations, particularly the detailed development level. The GAO agrees, and highlighted "human capitol management" as a high-risk, near-term concern.[493] Industry is the technological lead for IT, and the majority of government employees, be it government civilians or active duty members, cannot compete with that level of expertise, not for reasons of competence, but because their services are required for those "inherently government" functions, and IT changes so fast--one must be immersed in it everyday. Nor can Government service compete financially with the IT industry. It simply comes down to triage--the Government has only enough workers to fill these government functions. Industry can do the rest, and should do the rest, as they are immersed in it, and their life-blood is dependent on it. Embracing industry will certainly drive profits, and a new generation in a new service understands that profit is not a bad thing--it is not only the lifeblood that enable the freedoms the US enjoys but underpinning all the instruments of power--economic, military, informational, and political. *Profit is good*. Profiteering is not. The current generation does not understand the difference between the two. A new generation will if it is allowed to think differently. Profit is not unpatriotic. **It is capitalism.** By expanding the industry, investment in the private sector will help build on our own economic instrument of power, enable sophisticated protection mechanisms, and augment the industrial base to support information operations.

Congressman Davis' Technology Committee (discussed in Chapter 4) was formed in part to look at options concerning the "looming crisis in the information technology (IT) and acquisition workforces, as half of the IT workforce and one-third of the acquisition workforce will be eligible to retire in the next five years."[494] The Government recognizes "the impediments to attracting and retaining skilled technology and acquisitions workers." IT, under the auspices of the Government service, is not attractive, according to former U.S. Department of Labor Secretary Elaine Chao, who noted at a recent summit on the issue that:

> "America needs a wake-up call about its workforce. There will be huge economic consequences if we don't address demographic changes in the workforce and technological changes in the workplace . . . [t]he retirements of so many technology and acquisitions workers at precisely the same time we are having increasing difficulty in making government an employer of choice are challenges to good government that must be solved in the near future. [She went on to note that] the numbers are even more startling for the highly specialized fields where government is recruiting in direct competition with the private sector, and n**owhere is this more evident than with the technology workforce** [emphasis in original.]"[495]

The Sub-Committee went on to note that "Obtaining the best value for IT services requires a skilled acquisitions workforce . . [and that] [t]he current human resources management system for hiring, training, and retaining federal workers is not responsive to the diverse needs and wants of highly skilled IT and acquisition workers."[496] This mirrors the QDR concern, which noted the DoD has not kept pace with industry.

To preserve objectivity, note as well that the National Academy of Public Administration (NAPA), *is* more optimist than the author, and developed a four-part plan to incentivize government workers.[497] Their landmark report entitled *The Transforming Power of Information Technology: Making the Federal Government an Employer of Choice for IT Employees*, noted five key problems: 1) the government's human resources management system, 2) a "cumbersome recruiting process," 3) inadequate motivational tools, 4) poor learning opportunities, and 5) an accelerating pay gap."[498]

Being that an armed force is required, but that the industrial base is exceedingly dynamic, dispersed, and firmly rooted in the civilian sector, underpins the uniqueness of this new service construct--the DoD has no traditional structure, supporting the conclusions in Chapter 4 concerning dogmatic inflexibility. This new service would be composed of a small group of non-rated operations officers and cadre of enlisted personnel to "mage violence," heavily supported by industry.

This structure likewise follows Dr. Arnold Kanter's and Margiolli's recommendation as well. Dr. Kanter notes that

> "the Air Force should [perhaps] look outside the military into other complex government agencies and civilian organizations for models as well. High technology enterprises in the non-military sector might offer relevant inputs for USAF cohesion issues."[499]

Dr. Margiolli additionally notes that

> "support functions, removed from the flightline and silo, exhibited a more bureaucratic orientation and closer integration with civilian specialists, tending more toward occupational identifications. The highest technology areas of research and development, according to Margiotta, are indistin-

> guishable from civilian R&D institutions. In such an atmosphere, technology management is more prized than combat leadership."[500]

<u>Traditional Government Advisors.</u> It is prudent to likewise address the function of the traditional technical advisors that have served, and continue to serve the military establishment so well. These are the Federally Funded Research and Development Centers (FFRDC). An FFRDC is a "center that enables agencies to use private-sector resources to accomplish [R&D] tasks that are integral to agency missions and operations."[501] All FFRDCs are non-profit. "[They] are unique organizations] that assist the United States Government with scientific research and analysis, systems development, and systems acquisition.[502] The Government currently employs 36 FFRDCs--a Master List is maintained by the National Science Foundation (NSF). The Department of Defense and the Department of Energy comprise over 70% of the FFRDC customer base, with the DoD alone accounting for only 27%.

The different DoD military departments likewise use their FFRDCs in fundamentally different roles, and even the same service may employ its FFRDC support in an extremely dissimilar manner. For example, the USAF is heavily dependent on Aerospace Corporation for technical support to the space and missile community and assists the Government in systems development and systems acquisition.

The concern is that in developing an I-Service, largely predicated in the space and C3I communities will simply replicate the traditional FFRDC role. This may pose an insurmountable concern given the IT industry's concerns. An FFRDC, in order to discharge its responsibilities to the sponsoring agency has access beyond that which is common to the normal contractual relationship, including access to Government and supplier data, sensitive and proprietary data, and to employees and facilities. This, however, is one of the main concerns of the IT industry. Moreso than in any other market sector, proprietary data is the lifeblood of a company. The military simply does not understand this. A new service would, despite being chopped from various services that exist in this environment currently. It would be a new culture, a new organization.

Minimal FFRDC participation has a precedent in other services and in the Air Force as well. Interestingly enough, the FFRDCs are virtually absent in the aircraft community. Few FFRDCs are employed in aircraft development or air-to-air missile development, except for C2 interoperability. Even JASSM, an ACAT ID joint program, has no FFRDCs and relatively few SETAs. The Navy, uses its single FFRDC, the Center for Naval Analyses (CNA), in a fundamentally different role than does the Air Force as well. Whereas the USAF uses its FFRDC base mainly in acquisition with few employed in operational support, CNA's sole function is to improve operations, in direct support of the Chief of Naval Operations. CNA, which employs only 450-500 people, does not assist in the acquisition or system development, despite a similar--or in many cases greater--level of complexity in the USN's product base. The US Army relies on its main FFRDC, RAND Corporation, in yet a third role--that of policy development and for force structure shaping.

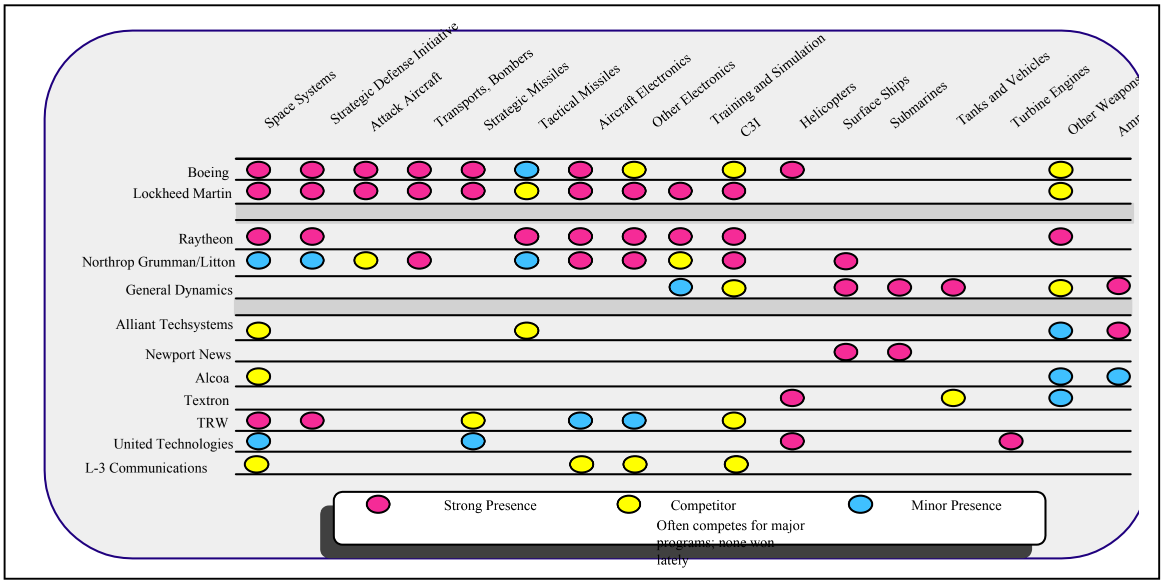
The Federal Acquisition Regulation (FAR), the document that contractually disciplines all government acquisitions, notes "an FFRDC may perform work for other than the sponsoring agency under the Economy Act, or other applicable legislation, when the work is not otherwise available from the private sector."[503] Finally, the FAR is also very clear that FFRDCs are only to be used for tasks where: "Existing alternative sources for satisfying agency requirements cannot effectively meet the special research or development needs."[504] FFRDCs are incredibly important and will remain so to the military because of their unique domain expertise and requisite objectivity. Aerospace Corporation for example, emerged as the analytical, technical, and programmatic underpinning that allowed the Air Force to militarize space, in that the space industry had no counterpart at the time. That is not longer the case--the commercial space industry is extremely broad, and well represented. The FFRDCs have served us well in this area, but industry now has the requisite experience as well.

Information, however, is the exact opposite. The computer industry far surpassed the DoD decades ago. The DoD is only a niche player. The same is true of communications. The military ushered in sophisticated C4I structures, centered on its huge communications monopoly as well as its computer edge. This too is no longer the case. One need look no further than Dell®. Within seconds of ordering a computer, Dell's inventory has been updated, replacements parts ordered, sales data trended, UPS notified for pickup and software vendors notified to begin to send the consumer updates to its software products--within seconds, all automatically. The DoD has no such counterpart and while it does not operate for a market economy, it too has an enormous logistics burden--requirements, supplies, replacement parts, and it requires mobilization, deployment, sustainment, and re-deployment.

Finally, IT expertise resides within the commercial sector. Therefore, the Government itself may face restrictions in using its FFRDCs in that

> "The sponsor, prior to extending the contract or agreement with an FFRDC, shall conduct a comprehensive review of the use and need for the FFRDC. . . where . . . the sponsor's special technical needs and mission requirements that are performed by the FFRDC to determine if and at what level they continue to exist [including] ". . . **consideration of alternative sources** to meet the sponsor's needs [emphasis added.]."[505]

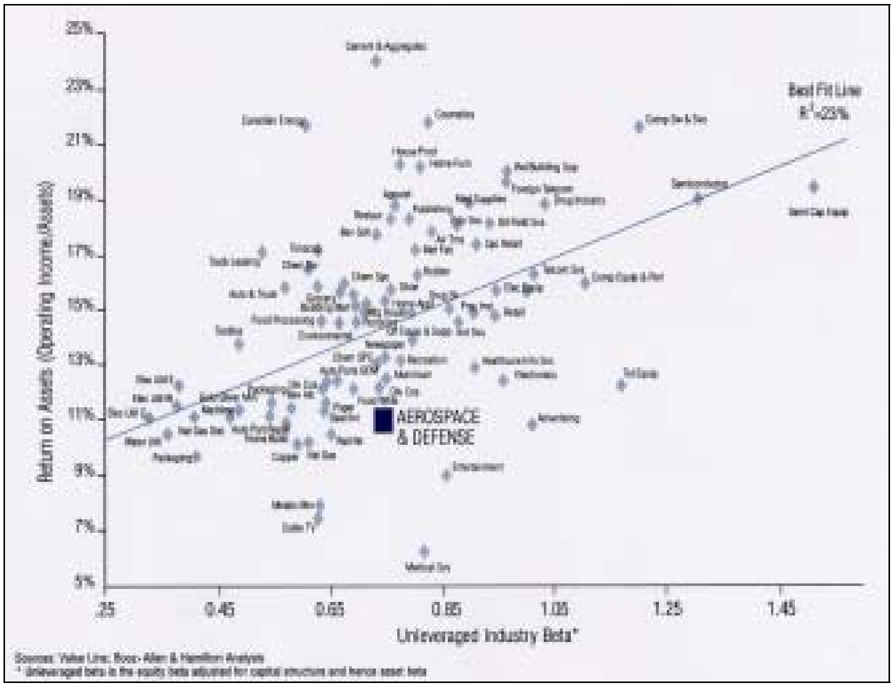
4. Have a significant industrial component and augmented industrial base. This section explains why simply using the DoD acquisition structure with respect to its industrial base is sub-optimal. That industry must be modified if a materiel solution is to be feasible. It is included to highlight the startling difference between the state of the industry in 1985 and present-day. Again, this is not the same DoD in which many of the current leadership, with their tales of $500 hammers and travel boondoggles, was borne. Much has been documented concerning the consolidation of the defense industry over the past two decades and its continuing evolution. Although some would contend it began with a dinner in 1993 hosted by then Secretary of Defense Les Aspin, subsequently dubbed "The Last Supper," where the Pentagon warned the heads of the largest defense contractors that defense spending would continue to decline--and in fact, accelerate in its decline--and that the Pentagon would not intercede with the resulting calculus of the de-



Source: "The Structure and Dynamics of the U.S. Defense Industry," Pierre A. Chao (26 Jan 01)

Figure 30: Broader Industrial Base But Fewer to Choose From

fense industry, the consolidation actually had begun seven years earlier when defense budgets began to plummet, losing ground with respect to overall percentage of the federal budget, as well as GDP. In fact, by 1993, most of the most significant consolidation had already been accomplished, in what Pierre Choa calls the first phase of consolidation as a function of conglomerate divestures.[506]



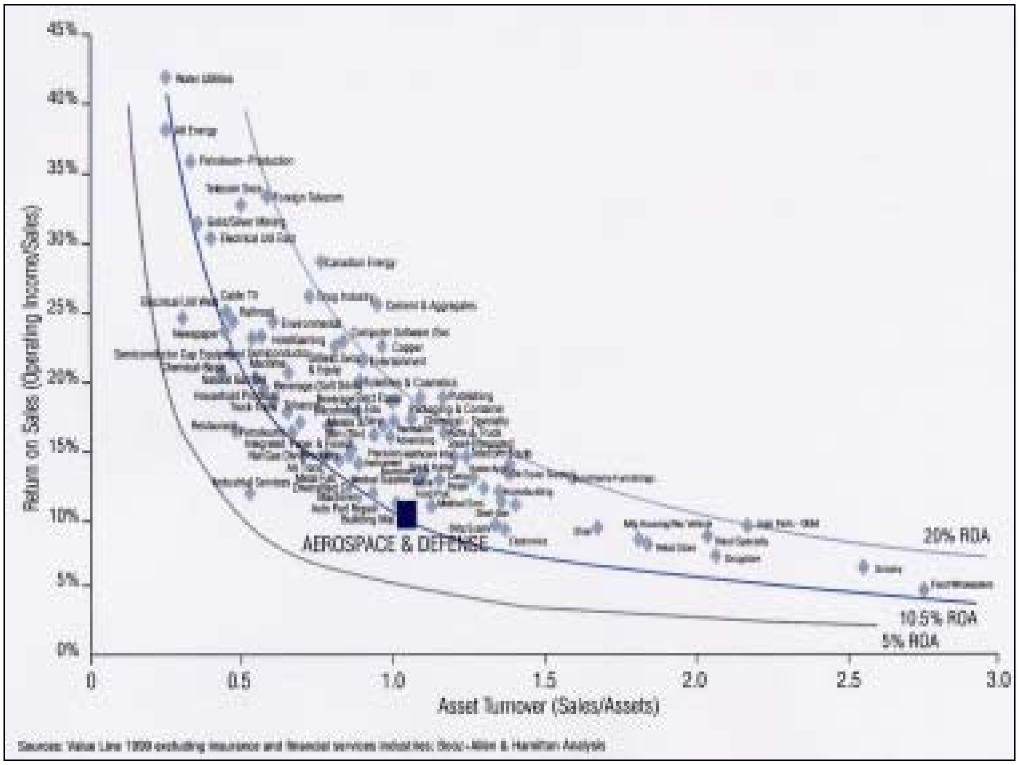
Sources: Value Line; Booz-Allen & Hamilton Analysis
* Unleveraged beta is the equity beta adjusted for capital structure and hence asset beta

Figure 31: Aerospace & Defense Industry Is Risk Prone with Sub-Average Profit Potential[507]

The defense industry has indeed significantly changed externally but internally as well, and while broader and more diversified, is weaker from a market perspective. This posture translates into more capable personnel migrating to higher payoff market sectors, and Wall Street disillusionment (Fig. 19). Wall Street does have a significant impact on DoD, and can affect everything from pay scales to bond ratings, to loan, acquisitions and mergers. The DoD industrial base is weaker than it was at the height of the Cold War. As shown in Fig. 20 this is a function mainly of Wall Street pressures and the growing service market.

Booz, Allen & Hamilton (BAH) cites the culpability of acquisition reform in terms of fewer competitions, the emergence of duopolies and triopolies forcing winner-loser acquisitions, and market consolidation forcing high debt.

> "The defense industry's combined operating profit has declined from 9.2% in 1996 to 7.7% in 1999, . . . the industry's collective interest coverage ratio has fallen 2.7 times in 1999 from 7.1 times in 1995 . . . and the industry's market capitalization is down 33% from $100.1B (Jan 1997) to $66.7B [in Jan 2000]. **As a whole, the industry's total value is 14% of Microsoft, 17% of Intel, 50% of AOL and 76% of Yahoo** [emphasis added.]."[34]



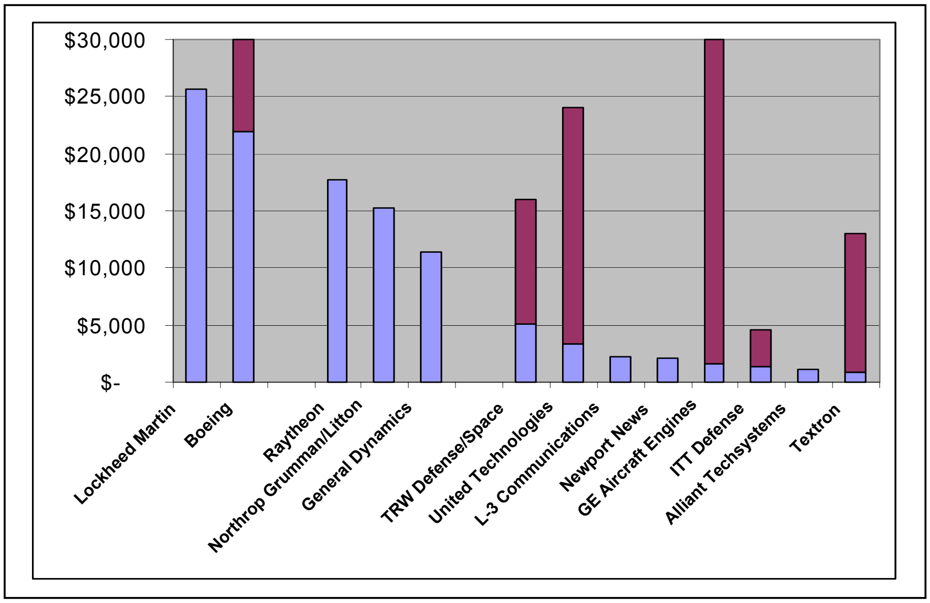
Sources: Value Line 1999 excluding insurance and financial services industries; Booz-Allen & Hamilton Analysis

Figure 32: Profitability in DoD Industrial Base Lower Than Less Risky Ventures[508]

In way of comparison, BAH notes that in a single day's market value appreciation of

Cisco Industries, one could buy the non-commercial components of Boeing, Lockheed-Martin, Raytheon, General Dynamics, Hughes, TRW, Northrop Grumman, Loral, and Litton, and still have $3B in your corporate account for investment in the Pharmaceutical and/or Biotechnology sectors, for example. Former Secretary of Defense Frank Carlucci, now chairman of Carlyle, a global equity investment partnership, notes as well that "the top ten defense companies had a capitalization less than Merk."[509]

As of Dec 2001, the nation's largest defense contractor was Lockheed-Martin. With an annual revenue of $25.3B, 60% of which comes from military contracts, its stock increased 73% since Jan 00, and traded at 26 times its expected earnings. L-M, however, continues to be burdened with a significant debt-capitol ratio of 62.4%.



Source: "The Structure and Dynamics of the U.S. Defense Industry," Pierre A. Chao (26 Jan 01)

Figure 33: Calculus of the Current DoD Industrial Base

Boeing is the nation's second largest defense contractor, but is heavily wed to the commercial aircraft industry. In fact, Boeing derives only 20% of its total annual revenue of $57B, from military sales. In addition, Boeing's debt-capitol ration is only 34%, half of its most aggressive competitor, Lockheed-Martin.

Raytheon, the nation's third largest defense contractor posted $16.9B in annual sales, 70% from military sales. Raytheon’s ’s debt-capitol ration is 38.8%. Raytheon may fair particularly well in the future given the increasing realization of the criticality of Information Operations, where Raytheon’s expertise lies, and will be remain well-poised for what Admiral Owens (ret), former Vice Chief of the Joint Chiefs of Staff, believes will be the next phase of warfare

The consolidation has resulted in far fewer providers, yet has provided a much more stable and more diversified internal corporate base, one better able to withstand the vacillations of the DoD budget--and one far more capable of supporting DoD’s diverse needs including pervasive R&D, and technical expertise. Yet even this broad base does not support a large IT emphasis. Of the three largest competitors, only Raytheon, which is smaller than either Lockheed-Martin or Boeing, as a significant IT background. New Government structures, acquisition policies, and leadership is needed to harvest civilian expertise. And new contractors are needed as well.

Therefore, unlike traditional USAF acquisition centers, the technical expertise of the I-Service would come from a new breed of contractors steeped in information powerhouses, for example, a Cisco. The traditional FFRDCs would revert to their technical origins centered on niche technology, long-term R&D (e.g. stealth, ultrasonics, acoustics, nanotechnology, etc.) and/or operational analysis. This is in line with the QDR that notes the “On the support side, the task is to remove layers that no longer provide.”[510]

One such approach would be to adopt commercial practices for IT development using end-product utility and emplacing Total System Performance Responsibility, a method which encourages minimum government oversight, with traditional and new contractor houses. Acquisitions would be executed under a trial system whereby the Congress would agree to freeze accounts for its top priority programs[511], encourage truth in acquisition cost, cap total costs, and freeze requirements. Information programs would then be locked, and built in blocks (taking advantage of the wisdom built into DoD 5000.1, 5000.2, and 5000.2R), with minimal government oversight, as is done in the corporate world (e.g. Pentium, Pentium II, III, IV, Windows 95, 98, 2000, XP, Acrobat Version 3.0, 3.1, 3.2, 4.0, etc.). This is not merely wishful thinking. The QDR demands acquisition revision noting both the "planning, programming and budgeting system (PPBS) and the acquisition process--create a significant amount of the self-imposed institutional work in the Department" and that the "DoD must explore options to fully redesign the way it plans, programs, and budgets."[512] As such, it is a mandate due to seven imitable and interoperable factors:

1. The necessity to further the weaponization of information,
2. The historical failures of C4ISR under the former construct,
3. The uniqueness of Major Acquisition Information Systems (MAIS) programs compared to other DoD acquisitions (as described in Chapter 4)
4. The dynamic nature of information
5. The history of software and communications technology products, which show multiple versions, locked, improved, and locked in a repetitive cycle,
6. No current service could adopt such far reaching changes within its own caste system
7. The QDR mandate to transform acquisitions

No service acquisition process meets all seven criteria. While all weapons would incorporate element #7 by default, none meet #3 and #4, or the accompanying inertia of a traditional kinetic weapon system. With strong support from Representative Davis, this trial program on a demonstrative basis would work, and is in keeping with the QDR's demands for necessary transformation and is in line with Secretary Aldridge's demand for "Acquisition Excellence" vice Acquisition Reform.

5. Develop a single acquisition center for C4ISR, space information systems, and intelligence products.

The QDR directs the DoD to develop recommendations to align, consolidate, or differentiate overlapping functions of the OSD, Services, and Joint Staff. This section provides one potential recommendation. It reviews those elements from the existing structure that must be re-organized to attain the level of efficiency the I-Service--and the nation--need. Proving that a service is necessary, outlining its basic construct, noting the significant industrial and civilian ties, still requires we draw upon a pool of Government talent to build that service's basic structure and begin to fill its ranks. The DoD needs to streamline, not expand. Creating another service without looking at existing functionality

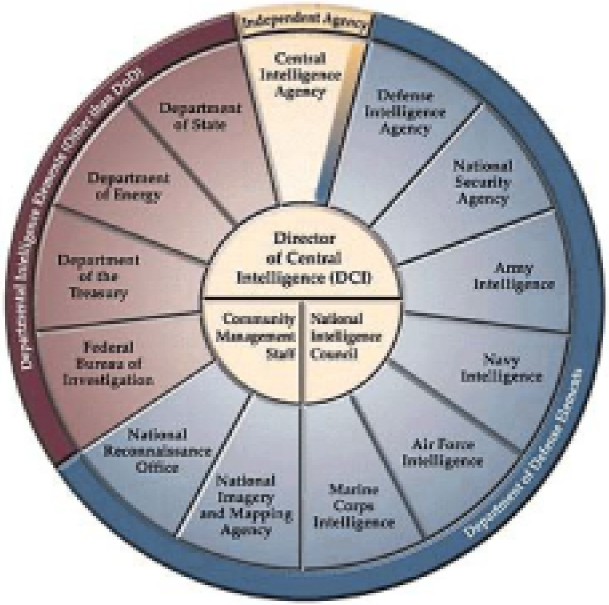

Independent Agency
Central Intelligence Agency
Defense Intelligence Agency
National Security Agency
Army Intelligence
Navy Intelligence
Air Force Intelligence
Marine Corps Intelligence
National Imagery and Mapping Agency
National Reconnaissance Office
Federal Bureau of Investigation
Department of the Treasury
Department of Energy
Department of State
Director of Central Intelligence (DCI)
Community Management Staff
National Intelligence Council
Departmental Intelligence Elements (Other than DoD)
Department of Defense Elements

Figure 34: The National Defense Intelligence Establishment, aka "the 13 tribes"[513]

would only exacerbate the very problem this research is trying obviate--integration, and new function sets. Today, intelligence is a vital element in every substantial international activity of the US government. The goal of intelligence is "to support decisionmakers with the best possible information, no matter its source."[514] To perform this continuous, monumental task, the Intelligence Community[515], headed by the CIA and collectively known as "the 13 tribes," gathers, interprets, and analyzes intelligence while preventing allies and adversaries from doing the same.[516]

One of the initial hypothesis of this paper was that many of the functions of the intelligence community, summarized in Table 16, could be better integrated and reduced. However, while significant integration is possible, and indeed necessary, the original desired breadth of integration does not appear to be possible upon further investigation, with two exceptions: 1) True consolidation, 2) Transposing existing functions. With respect to the latter, the NRO, DAI, NSA and the four service intelligence agencies should be integrated under the I-Service. **An additional service intelligence agency should likewise be added for Special Operations to aid the non-regionalized communications necessary for a asymmetric warfare conducted by multiple cells dispersed world-wide.** The support provided by HUMINT, ground, manned and unmanned platforms, and future unmanned, remotely controlled sensors (e.g. acoustic, positional, etc.) sensors, must be horizontally integrated vice remaining in their traditional stovepipes. The NRO in particular, being solely focused on **space** ISR efforts, i.e. geographically-based and structured around Euclidean demarcations--would fall instead under the I-Service, for the reasons stated in Chapter 3--namely, these assets are simply conduits for information. The current construct is simply too narrowly focused given the changing international environment and the declassification of many of its functions and its systems. Keith Hall, then the director of the NRO noted that one of the reasons for declassifying the existence of some of the NRO function s and systems was in fact to break down traditional security barriers for the benefit of the national interest. This migration may well concern the CIA, NRO’s largest customer. However, the CIA needs *data*, *information* and/or ultimately intelligence, and a single entity, can best provide these. As such, the other services intelligence functions would not completely disappear, but would become liaison offices within the I-Service. Finally, DISA, controlling the information conduit, would also be subsumed by the I-Service, where it could manage its military communication responsibilities.

Table 16: Optimizing the 13 Tribes

ORGANIZATION	I-Service Absorb/ Re-organize Function?	Current Function
Central Intelligence Agency (CIA) [517]	**No.** **Why Not?** **- Constitutional constrains** **- Retain Civilian Control.** **- Posse Comitatus**	• Providing accurate, comprehensive, and timely foreign intelligence on national security topics • Conducting counterintelligence activities, special activities, and other functions related to foreign intelligence and national security, as directed by the President. • CIA collects foreign intelligence information through a variety of clandestine and overt means. The Agency also engages in research, development, and deployment of high-leverage technology for intelligence purposes • In addition to these activities, CIA contributes to the effectiveness of the overall Intelligence Community by managing services of common concern in imagery analysis and open source collection, and by participating in strategic partnerships with other intelligence agencies in the areas of research and development and technical collection.
The Defense Intelligence Agency (DIA) [518]	**Yes.** **All Source Intelligence** ***a priori* architecting**	• Designated Combat Support Agency and the senior military intelligence component of the Intelligence Community. • DIA's primary mission is to provide all-source intelligence to the US armed forces. • Plays a key role in providing information on foreign weapons systems to US weapons planners and the weapons acquisition community. • Coordinates and synthesizes military intelligence analysis for Defense officials and military commanders worldwide

Table 16: Optimizing the 13 Tribes

ORGANIZATION	I-Service Absorb/ Re-organize Function?	Current Function
National Security Agency (NSA) [519]	**Yes.** **- Currently Stovepiped** **- Better MASINT product**	• NSA plans, coordinates, directs, and performs foreign signals intelligence (SIGINT) and information security (INFOSEC) functions.
Army Intelligence[520]	**- Yes** **- Retain Liaison function**	• Army's assets provide commanders with the capability to communicate with and receive intelligence from many intelligence agencies. • Provide timely, relevant, accurate and synchronized intelligence and electronic warfare support to tactical, operational and strategic level commanders across the range of Joint military operations • Has a robust intelligence structure that supports tactical level warfighters.
Naval Intelligence[521]	**- Yes** **- Retain Liaison function**	• support the operating forces, the Department of the Navy, and the maritime intelligence requirements of national level agencies. • the principal source for maritime intelligence on global merchant affairs and a national leader in other non-traditional maritime issues
Air Force Intelligence, Surveillance, and Reconnaissance[522]	**- Yes** **- Retain Liaison function**	◆ Focused on ensuring the US military team - whether in peacetime operations, a crisis, or war - attains information superiority: the ability to collect, control, exploit, and defend information while denying the adversary the ability to do the same ◆ Air Force ISR fills a variety of roles to meet the US' national security requirements.

Table 16: Optimizing the 13 Tribes

ORGANIZATION	I-Service Absorb/ Re-organize Function?	Current Function
Marine Corps Intelligence[523]	- Yes - Retain Liaison function	◆ Provides services and specialized products to support the Commandant of the Marine Corps as a member of the Joint Chiefs of Staff, as well as to the Marine Corps Headquarters Staff. ◆ Marine Intelligence supports acquisition policy and budget planning and programming, and provides pre-deployment training and force contingency planning for requirements that are not satisfied by theater, other service, or national capabilities.
Special Operations Intelligence	- New - Better track non-regionalized threats with foreknowledge of Special Operations Capabilities	◆
National Imagery and Mapping Agency (NIMA) [524]	- Yes - Continue consolidation of intel product and find better ways to get it to the field without compromising the source	◆ Provides timely, relevant, and accurate imagery, imagery intelligence, and geospatial information in support of military, national-level, and civil users. ◆ Merged the previously separate disciplines of imagery and mapping has assumed leadership of the imagery and geospatial community
The National Reconnaissance Office (NRO) [525]	- Yes - Currently stovepiped for space only ISR. - Better cross-flow critical with maturation of UAVs, Rivet Joint, JSTARS, and potential tanker assets	◆ The single, national program to meet US government needs through spaceborne reconnaissance. ◆ Ensure that the US has the technology and spaceborne assets needed to enable US global information superiority. ◆ Collect intelligence to support such functions as indications and warning, monitoring of arms control agreements, military operations and exercises, and monitoring of natural disasters and other environmental issues.

Table 16: Optimizing the 13 Tribes

ORGANIZATION	I-Service Absorb/ Re-organize Function?	Current Function
Federal Bureau of Investigation (FBI)[526]	**No.** **Why Not?** **- Retain Civilian Control.** **- Posse Comitatus**	◆ Uphold the law through the investigation of violations of federal criminal statutes ◆ Protect the United States from hostile intelligence efforts ◆ Provide assistance to foreign and other US federal, state, and local law enforcement agencies ◆ Perform these responsibilities in a manner that is faithful to the Constitution and laws of the United States.
Office of Intelligence Support[527]	**No.** **Why Not?** **- Retain Civilian Control.** **- Posse Comitatus** **- Preserve independence of Economic IOP**	◆ Official responsible for the integrity of the country's currency ◆ Focal point on intelligence matters for the Department and Community agencies ◆ Responsible for providing timely, relevant intelligence to the Secretary and other Treasury Department officials
Department of Energy[528]	**No.** **Why Not?** **- Retain Civilian Control.** **- Infrastructure critical WRT US vulnerabilities**	◆ Contribute to the welfare of the nation by providing the scientific foundation, technology, policy, and institutional leadership necessary to achieve efficiency in energy use, diversity in energy sources, a more productive and competitive economy, improved environmental quality, and a secure national defense. ◆ Provide the Department and other US Government policymakers and decisionmakers with timely, accurate, high-impact foreign intelligence analyses ◆ To detect and defeat foreign intelligence services bent on acquiring sensitive information on the Department's programs, facilities, technology, and personnel
Bureau of Intelligence and Research[529]	**Yes.** **- Track non-regionalized threats**	◆ Primary source for interpretive analysis of global developments. ◆ Providing the Secretary and other key decisionmakers with expert, independent foreign affairs analysis ◆ Coordinates the handling of issues that arise in the course of intelligence, security, counterintelligence, investigative, ~~and special operations~~. (move to New SO cell)
Combatant Forces	**New**	◆ Provide trained and equipped forces to CINCs for weapon execution
C4 Cell	**New**	◆ Align C4ISR acquisitions ◆ Mange C4 acquisitions

Source: “Unites States Intelligence Community.”

The three C2 centers, Electronic Systems Command at Hansom AFB, MA, Space and Naval Warfare Systems Command (SPAWAR) in San Diego, CA and the Army's Communications Electronic Command (CECOM) at Fort Belvoir, VA would be consolidated under the I-Services Services. As shown in Chapter 4, these forces each build C4ISR systems--but their focus is on their own service. RAND largely supports CECOM through analysis, Mitre supports ESC through technical development, oversight, and management, and CNA only evaluates the interoperability of the C4ISR systems developed for the Navy. Again, the I-Service would be largely integrated with industry, with some forces constantly engaged in a military duties, others deployable, and still others, largely immersed in evolving the civilian technology into military counterparts.

This consolidation, however, amounts to little more than organizational restructure. What must accompany this transformation is a unifying vision, unifying leadership, and ties to the IT industry that has far surpassed the military. And it must remain firmly rooted in civilian control with maximum protection of American civil rights, but balanced with the maturity necessary given America's open society and global impact..

Notes

[476] Potential Materiel Alternatives. Identify known systems or programs addressing similar needs that are deployed or are in development or production by any of the Services, agencies, or allied nations. Discuss the potential for inter-Service or allied cooperation. Indicate potential areas of study for concept exploration, including the use of existing US or allied military or commercial systems, including modified commercial systems or product improvements of existing systems." (See: CJCS 3170.01B. *Requirements Generation System*, 15 Apr 2001, C-A-1.)

[477] "The Posse Comitatus Act: A Principle in Need of Renewal." *Washington University Quarterly*. (Volume 75. Summer 1997 No. 2.), 1.

[478] Booz, Allen & Hamilton. "US Defense Industry Under Siege--An Agenda for Change," December 1999. On-line. Internet. Available from: www.aerospacelinks.com.

Notes

[479] "Epic cyberattack reveals cracks in U.S. defense." CNN/Sci-tech.com, 10 May 2001, n.p. On-line. Internet, 20 December 2002. Available from http://www.cnn.com/2001/tech/Internet/05/10/3.year.cyberattacck.idg/index.html.

[480] "The Posse Comitatus Act," 6.

[481] "POSSE COMITATUS ACT" (18 USC 1385): A Reconstruction Era criminal law proscribing use of Army (later, Air Force) to "execute the laws" except where expressly authorized by Constitution or Congress. Limit on use of military for civilian law enforcement also applies to Navy by regulation. Dec '81 additional laws were enacted (codified 10 USC 371-78) clarifying permissible military assistance to civilian law enforcement agencies--including the Coast Guard--especially in combating drug smuggling into the United States. Posse Comitatus clarifications emphasize supportive and technical assistance (e.g., use of facilities, vessels, aircraft, intelligence, tech aid, surveillance, etc.) while generally prohibiting direct participation of DoD personnel in law enforcement (e.g., search, seizure, and arrests). [emphasis added]. (See, "The Posse Comitatus Act," 6.)

[482] The PCA criminalizes, effectively prohibiting, the use of the Army or the Air Force as a posse comitatus [11] to execute the laws of the United States. It reads: "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both." See: ?

[483] Secretary of the Treasury Alexander Hamilton envisioned a unique maritime service in 1787, when he proclaimed, "A few armed vessels, judiciously stationed at the entrances of our ports, might at a small expense be made useful sentinels of our laws." The scope of the responsibility began to grow, and it was clear that "more than just a few armed vessels stationed at the entrances of our ports would be required to ensure America's security." See: ?

[484] "US Coast Guard. The Essence of the Coast Guard: America's Maritime Guardians." In *Joint Force Employment Coursebook Academic Year 2002*. Compiled by Col(s) James Forsyth Jr., PhD, et al. Air Command and Staff College: Department of Joint Warfare Department. Maxwell, AFB, AL. Aug 2001, 24.

[485] US Government. "Inherent Government Functions." PDD 92-1.

[486] Costa, Robert. "FFRDCS Evolution As a function of Changing DoD Calculus." Unpublished. Defense Systems Management College, Fort Belvoir: VA, 3 Auf 2002, n.p.

[487] QDR, 61.

[488] QDR, 62.

[489] QDR, 62.

[490] QDR, 61-2.

[491] "Epic cyberattack reveals cracks in U.S. defense." CNN/Sci-tech.com, 10 May 2001, n.p. On-line. Internet, 20 December 2002. Available from http://www.cnn.com/2001/tech/Internet/05/10/3.year.cyberattacck.idg/index.html.

Notes

[492] Khalilzad, Aalmay M. and John P. White. Strategic Appraisal: The Changing Role of Information in Warfare. (RAND: Project Air Force. Santa Monica, CA) 1999. 62-3.

[493] US House. HEARING NOTICE: Transforming the IT and Acquisition Workforces: Using Market-Based Pay, Recruiting and Retention Strategies to Make the Federal Government an Employer of Choice for IT and Acquisition Employees. 101st Congress, Subcommittee on Technology and Procurement Policy, 2 Oct 01. n.p.

[494] Ibid.

[495] Ibid.

[496] Ibid.

[497] The legislation has four primary components. First, it creates a market-based, pay-for-performance system for those federal IT and acquisitions workers who want to derive the benefits and undertake the responsibilities of such as system. Second, it enables flexible and improved recruiting and hiring processes by bringing the new class of employees in as excepted service, non-career employees who can be hired far more quickly than is commonly possible under traditional career and career-conditional appointments. Third, the legislation expands work/life options and other competitive benefits by building on the federal government's recognized success in offering attractive working conditions. In an environment where pay cannot always match the market rate, government needs to consider what creatively applied benefits may tilt the balance in favor of employment with a federal agency. Finally, it helps make the government's training and education opportunities second to none. (See: US House. HEARING NOTICE.)

[498] US House. HEARING NOTICE.

[499] Smith, James M. "USAF Culture and Cohesion: Building and Air and Space Force for a 21st Century." Institute for National Strategic Studies. Occasional Paper 19. Colorado Springs, CO: USAF Institute for National Security Studies, June 1998.

[500] Ibid.

[501] Mitre Homepage, 1 May 2001. On-line. Internet, 28 February 2002. Available from www.mitre.org.

[502] "FFRDCs meet some special long-term research or development need which cannot be met as effectively by existing in-house or contractor resources. FFRDCs enable agencies to use private sector resources to accomplish tasks that are integral to the mission and operation of the sponsoring agency. The FFRDC is required to conduct its business in a manner befitting its special relationship with the Government, to operate in the public interest with objectivity and independence, to be free from organizational conflicts of interest." FFRDCs were established in the years just prior to and during WWII and many are celebrating 40 and 50 year anniversaries. "[They] work in the fields of defense, energy, aviation, space, health and human services, and tax administration. See:

[503] Federal Acquisition Regulation. On-line. Internet, 7 March 2002, n.p. Available from http://www.arnet.gov/far/, 35.0-7.

[504] Ibid.

[505] Ibid, 35.0-8.

Notes

[506] Chao, Pierre A. "The Structure and Dynamics of the U.S. Defense Industry." Lecture, 18 July 2001. Defense Systems Management College, Fort Belvoir: VA, 26 Jan 2001, 12.)

[507] "Standard & Poor's Industry Surveys." www.sp.com, 15 February 2001, n.p.Online. Internet,15 July 2001.Available by subscription only.

[508] "Standard & Poor's Industry Surveys." www.sp.com, 15 February 2001, n.p.Online. Internet,15 July 2001.Available by subscription only.

[509] "Ex-pentagon chief targets Defense." 12 Feb 01, n.p. www.Barron.com. On-line. Internet, 12 Jul 2002. Available from www.publiceye.org/frontpage/911/boin.html.

[510] QDR, 51.

[511] This method was used in at the Air Force Research Laboratory in 1998-2001, whereby the top priority programs funding was stabilized and not subject to the perennial funding cuts. Several smaller programs, absorbing the majority of cuts were eliminated, while critical programs, including Communication/Navigation Outage Forecasting Satellite (C/NOFS) and MightySat II.1 (*Sindri*) were finally able to concentrate resources on completing the program. It worked. *Sindri* flew the first DoD hyperspectral imager, and C/NOFs became the #1 priority program at the Space Experiment Requirements Board.

[512] QDR, 51.

[513] "Unites States Intelligence Community." www. cia.gov, 15 June 1998, n.p. Online. Internet, 30 November 2001. Available from http://www.cia.gov/ic/icagen2.htm

[514] Ibid.

[515] A series of statutes and Executive Orders provides legal authority for the conduct of intelligence activities. Key documents include the National Security Act of 1947 (as amended), which provides the basic organization of the US's national security effort, and Executive Order 12333, which provides current guidelines for the conduct of intelligence activities and the composition of the Intelligence Community. (See: US Intelligence Community.")

[516] "Unites States Intelligence Community."

[517] "Unites States Intelligence Community." www. cia.gov, 15 June 1998, n.p. Online. Internet, 30 November 2001. Available from http://www.cia.gov/ic/icagen2.htm.

[518] Ibid.

[519] Ibid.

[520] Ibid.

[521] Ibid.

[522] Ibid.

[523] Ibid.

[524] Ibid.

[525] Ibid.

[526] Ibid.

[527] Ibid.

[528] Ibid.

[529] Ibid.

Glossary

ACC	Air Combat Command
ACSC	Air Command and Staff College
ACTS	Air Corps Tactical School
AEF	Aerospace Expeditionary Forces
AEG	Aerospace Expeditionary Group
AESA	Active Electronically Scanned Array Radar
AETC	Air Education and Training Command
AEW	Aerospace Expeditionary Wing
AFDD	Air Force doctrine document
AFSCN	Air Force Satellite Control Network
AFSPC	Air Force Space Command
AOR	Area of responsibility
ASAT	Anti-Satellite
AU	Air University
BAH	Booz, Allen & Hamilton
C2W	Command and Control Warfare
C4ISP	Command and Control, Computers and Communications, Intelligence Support Plan
C4ISR	Command, Control, Communications, Computers, Intelligence,
CECOM	Communications Electronic Command
CERT	Computer Emergency Response Team
CI	Counterinformation
CIPO	C2 integrated Program Offices
CNA	Computer Network Attack
CND	Computer Network Defense
COG	Center of Gravity
CSAF	Chief of Staff of the US Air Force
CW	Cyber Warfare
DCA	Defensive CounterAir
DCI	Defensive CounterInformation
DIA	Defense Intelligence Agency
DIE	Defense Intelligence Establishment
DoD	Department of Defense

Glossary

DP	Decisive Point
DPG	Defense Planning Guidance
DSCS III	Defense Satellite Communications System Phase III
DSMC	Defense Systems Management College
EAF	Expeditionary Aerospace Force
EASTPAC	Eastern Pacific Defense Satellite Communications System
EFX	Expeditionary Air Force Exercise
EM	Electromagnetic
EP	*Exclusivity-Primary*
ES	*Exclusivity Secondary*
ESC	Electronic Systems Command
EW	Electronic Warfare
EWO	Electronic Warfare Officer
FAR	Federal Acquisition Regulation
FFRDC	Federally Funded Research and Development Corporation
GCS	Ground Control Station
GDP	Gross Domestic Product
GH	Global Hawk
GO	General Officer
GPS	Global Positioning System,
HARM	High-Speed Anti-Radiation Missile
HUMINT	Human Intelligence
IA	Information assurance
IA	Information Attack
IADS	Integrated Air Defense System
IGF	Inherent Government Function
IIW	Information-in-Warfare
INFOSEC	Information security
INSS	Institute for National Security Studies
IO	Information operations
IOP	Instrument of Power
IR&D	Independent Research and Development
IS	Information Superiority
I-Service	Information-Service
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
ITO	In Terms Of
IW	Information Warfare
JADM	Joint Direct Attack Munitions
JP	Joint Publication
JSASSM	Joint Air-to-Surface Standoff Missile
JSF	Joint Strike Fighter
JTF	Joint Force Commander
KPP	Critical Performance Parameter

KW	Kilowatt
LRAPP	Long Range Air Power Panel
MAIS	Major Automated Information Systems
MASINT	Measures and Analysis Intelligence
MDAP	Major Defense Acquisition Program
MNA	Mission Needs Analysis
MNS	Mission Needs Statement
MOOTW	Military Operations Other Than War
MTW	Major Theater of War
N/UWSS	NORAD/USSPACECOM Warfighting Support System
NAIC	National Air Intelligence Center
NMS	National Military Strategy
NPIC	National Infrastructure Protection Center
NRO	National Reconnaissance Office
NSP	Network Service Provider
NSS	National Security Strategy
NSS	National Security System
OCA	Offensive CounterAir
OCI	Offensive CounterInformation
ODF	Operation Deliberate Force
OEF	Operation Enduring Freedom
OHS	Office of Homeland Security
OODA	Observe, Orient, Decide, Act
ORD	Operation Restore Democracy
ORH	Operation Restore Hope
PDD	Presidential Decision Directive
PGM	Precision Guided Munitions
PME	Professional Military Education
PPBS	Planning, Programming and Budgeting System
PSTN	Public Switched Telephone Network
QDR	Quadrennial Defense Review
RTB	Radar Test Bed
SAAS	School of Advance Airpower Studies
SAR	Special Access Required
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communication
SEAD	Suppression of Enemy Air Defenses
SECAF	Secretary of the Air Force

Glossary

SIGINT	Signals Intelligence
SPAWAR	Space and Naval Warfare Systems Command
SPD5	Surveillance, Protection Deny, Disrupt, Destroy, Deceive, Degrade
SSN	Space Surveillance Network
STO	Space Tasking Order
TBMCS	Theater Battle Management Core System
UAV	Uninhabited Arial Vehicle
UoA	Unity of Action
UoC	Unity of Command
UoE	Unity of Effort
USCG	US Army Command and General Staff College
WRT	With Respect To

Definitions

Automated Information System (AIS). An acquisition program that acquires Information Technology (IT), except IT that:Involves equipment that is an integral part of a weapon or weapons system; or Is a tactical communication system.

Capstone Requirements Document. A document that contains performance-based requirements to facilitate development of individual operational requirements documents by providing a common framework and operational concept to guide their development.

Command and control warfare. The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the operational continuum and at all levels of conflict. Also called C2W. C2W is both offensive and defensive: a. counter-C2ŠTo prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2- protect tion. To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. (Joint Pub 1-02)

computer intrusion. An incident of unauthorized access to data or an automated information system.

computer intrusion detection. The process of identifying that a computer intrusion has been attempted, is occurring, or has occurred.

computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack (CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using and electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA. (JP 3-51)

computer network defense. Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. (JP 3-51)

computer security. The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 6-02)

data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned

defensive information operations. The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes.

doctrine. Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application.

electromagnetic jamming. The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effecttive use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability.

electromagnetic spectrum. The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands.

electronic warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a.electronic attack. That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. electronic protection. That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. c. electronic warfare support. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (JP 3-51)

Family of Systems. A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation (GL-8)

Hoax. Usually an email that gets mailed in chain letter fashion describing some devastating highly unlikely type of virus, you can usually spot a hoax because there's no file attachment, no reference to a third party who can validate the claim and the general 'tone' of the message.

Information. 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 3-13.1)

information assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 3-13)

information attack. An activity taken to manipulate or destroy an adversary's information systems without visibly changing the physical entity within which it resides. (Air Force term as applied to the scope of this AFDD.)

information dominance. the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations other than war while denying those capabilities to the adversary (Army Definition)

information environment. The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (JP 3-13)

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. (JP 3-13)

Information Operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems information operations: Continuous military operations within the military information environment that enable, enhance, and protect the friendly forceís ability to collect, process, and act on information to achieve an advantage across the full range of military operations; information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities Army Definition

information report. Report used to forward raw information collected to fulfill intelli gence requirements.

information requirements. Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander.

information security. The protection of information and information systems against unauthorized access or modification of information, whether in storage, proc essing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and com munications security.

information Superiority. That degree of dominance in the information domain which permits the conduct of operations without effective opposition

information system. The entire infrastructure, organization, personnel, and components hat collect, process, store, transmit, display, disseminate, and act on information. (JP 3-13)

information systems security. A composite means to protect telecommunications systems and automated information systems and the information they transmit and/or process

Information Technology (IT). Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

information warfare. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (JP 3-13)

information warfare. Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending oneís own information, information-based processes, information systems and computer-based networks (**CJCSI 3210.01**)

information-in-warfare. Involves the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on integrated intelligence, surveillance, and reconnaissance (ISR) assets; information collec tion/dissemination activities; and its global navi-gation and positioning, weather, and communications capabilities.

infosphere. The rapidly growing global network of military and commercial command, control, communications, and computer systems and networks linking information data bases and fusion centers that are accessible to the warrior anywhere, anytime, in the performance of any mission; provides the worldwide automated infor mation-of-exchange backbone support to joint forces; and provides seamless operations from anywhere to anywhere that is secure and transparent to the warrior; this emerging capability is highly flexible to support the adaptive com mand and control infrastructures of the twenty-first century (Army Definition)

interoperability. 1. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. 2. (DOD only) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases.

joint doctrine. Fundamental principles that guide the employment of forces of two or more Military Departments in coordinated action toward a common objective. It is authoritative; as such, joint doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. It will be promulgated by or for the Chairman of the Joint Chiefs of Staff, in coor dina tion with the combatant commands and Services

Joke. A harmless program that causes various benign activities to display on your computer (e.g., an unexpected screen-saver).

Major Automated Information System (MAIS. An AIS that is designated by ASD(C3I) as a MAIS, or estimated to require program costs in any single year in excess of $32 million in fiscal year (FY) 2000 constant dollars, total program costs in excess of $126 million in FY 2000 constant dollars, or total life-cycle costs in excess of $378 million in FY 2000 constant dollars.

Major Defense Acquisition Program (MDAP). An acquisition program that is not a highly sensitive classified program (as determined by the Secretary of Defense) and that is designated by the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) as an MDAP, or estimated by the USD(AT&L) to require an eventual total expenditure for research, development, test and evaluation of more than $365 million in fiscal year (FY) 2000 constant dollars or, for procurement, of more than $2.190 billion in FY 2000 constant dollars.

Major System. A combination of elements that shall function together to produce the capabilities required to fulfill a mission need, including hardware, equipment, soft ware, or any combination thereof, but excluding construction or other improvements to real property.

Mission Critical Information System. A system that meets the definitions of "in formation system" and "national security system" in the Clinger-Cohen Act, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical should be made by a Component Head, a CINC or their designee.) A Mission Critical Infor mation Technology System has the same meaning as a Mission Critical nformation ystem.

Mission Essential Information System. A system that meets the definition of "informa tion system" in the Clinger-Cohen Act, that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organ izational mission. (Note: The designation of mission essential should be made by a Component Head, a CINC or their designee.) A Mission Essential Information Technology System has the same meaning as a Mission Essential Information Sys tem.

National Security System (NSS). Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which:Involves intelligence activities; Involves cryptologic activities related to national security; Involves command and control of military forces; Involves equipment that is an integral part of a weapon or weapons system; or, subject to the limitation below, is critical to the direct fulfillment of military or intelligence missions. This does not include a system that is to be used for routine administrative and business appli cations (including payroll, finance, logistics, and personnel management applications)

offensive information operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers to achieve or promote specific objectives. These capabilities and activities include but are not limited to operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could also include computer network attack.

offensive information operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers to achieve or promote specific objectives. These capabilities and activities include but are not limited to operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could also include computer network attack.

Operational Requirements Document. A formatted statement containing performance and related operational parameters for the proposed concept or system. Prepared by the user or user's representative at each milestone beginning with Milestone I, Concept Demonstration Approval of the Requirements Generation Process.

Posse Comitatus Act. (Source: G-OPL)"POSSE COMITATUS ACT" (18 USC 1385): A Reconstruction Era criminal law proscribing use of Army (later, Air Force) to "execute the laws" except where expressly authorized by Constitution or Congress. Limit on use of military for civilian law enforcement also applies to Navy by regulation. Dec '81 additional laws were enacted (codified 10 USC 371-78) clarifying permissible military assistance to civilian law enforcement agencies--including the Coast Guard--especially in combating drug smuggling into the United States. Posse Comitatus clarifications emphasize supportive and technical assistance (e.g., use of facilities, vessels, aircraft, intelligence, tech aid, surveillance, etc.) while generally prohibiting direct participation of DoD personnel in law enforcement (e.g., search, seizure, and arrests). For example, Coast Guard Law Enforcement Detachments (LEDETS) serve aboard Navy vessels and perform the actual boardings of interdicted suspect drug smuggling vessels and, if needed, arrest their crews). Positive results have been realized especially from Navy ship/aircraft involvement.

space control operations. Operations that provide freedom of action in space for friendly forces while, when directed, denying it to an enemy, and include the broad aspects of protection of US and US allied space systems and negation of enemy space systems. Space control operations encompass all elements of the space defense mission.

space support operations. Operations required to ensure that space control and support of terrestrial forces are maintained. They include activities such as launching and deploying space vehicles, maintaining and sustaining space vehicles while on orbit, and recovering space vehicles if required

space systems. All of the devices and organizations forming the space network. The network includes spacecraft, ground control stations, and associated terminals.

space weather. A term used to describe the environment and other natural phenomena occurring above 50 kilometers altitude that can degrade Department of Defense communications (satellite communications and skywave), global positioning system, radar, and satellite operations.

special information operations. Information operations that by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. (JP 3-13)

System-of-Systems. A set or arrangement of systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole. (G-14)

Trojan Horse. A program that neither replicates or copies itself, but does damage or compromises the security of the computer. Typically it relies on someone emailing it to you, it does not email itself, it may arrive in the form of a joke program or software of some sort.

Virus. A program or code that replicates, that is infects another program, boot sector, partition sector or document that supports macros by inserting itself or attaching itself to that medium. Most viruses just replicate, a lot also do damage.

Worm. A program that makes copies of itself, for example from one disk drive to another, or by copying itself using email or some other transport mechanism. It may do damage and compromise the security of the computer. It may arrive in the form of a joke program or software of some sort.

Bibliography

"'Code Red' impact felt at major companies." CNN.com, 9 August 2001, n.p. On-line. Internet, 20 December 2001. Available from http://www.cnn.com/2001/TECH/internet/08/09/code.red/.

"ACSC Research Project 95-053: Planning and Execution of Conflict Termination." In Air Command and Staff College Distance Learning Program. Lesson Wc503r05. CD-ROM ACSC Multimedia Edited Version 2.2., Aug 1997, n.p.

"Advance Questions for General John P. Jumper Nominee for the Position of Chief of Staff of the United States Air Force," US Senate Armed Services Committee, 8 January 2001, n.p. On-line. Internet, 20 February 2002. Available from www.senate.gov/~armed_services/statemnt/2001/ a010801 jumper.pdf.

Albaugh, James F.. "Space and the Fight Against Terrorism." *Space News*. 20 May 2002.

"Analyst estimates Internet virus hit eight million systems." ABC News Online, 3 October 2001, n.p. On-line. Internet, 20 December 2001. Available from http://www.abc.net.au/news/science/computers / 2001 /10/item20011003022605_1.htm.

"Bin Laden says US Economy Was Target." CNN.com, 28 December 2001, n.p. On-line. Internet, 3 February 2002. Available from http://www.cnn.com/2001/WORLD/asiapcf/central/12/27/ ret.bin.laden.tape/.)

"Cannae Toolbook Text." In Air Command and Staff College Distance Learning Program. Lesson TH504r02. CD-ROM ACSC Multimedia Edited Version 2.2., Aug 1997, n.p.

"CERT® Advisory CA-2001-26 Nimda Worm." CERT.org, 25 Sep 2001, n.p. On-line. Internet,. 20 December 2001. Available from http://www.cert.org/advisories/CA-2001-26.html.

"China Extracts Computer-Virus Samples." Wall Street Journal, 30 March 2001

"China Threatens 'Electronic Pearl Harbor' Attack on U.S." Infowar.com, 11 October 2000, n.p. On-line. Internet, 6 January 2002. Available from http://www.Infowar.com/mil_c4i/00/ mil_c4i_101100b_j.shtml.

"Contractors Target New Technologies -- And Each Other." Washington Post. 23 February 23, 2002, n.p.

"Epic cyberattack reveals cracks in U.S. defense." CNN/Sci-tech.com, 10 May 2001, n.p. On-line. Internet, 20 December 2002. Available from http://www.cnn.com/2001/tech/Internet/05/10/3.year.cyberattacck.idg/index.html.

"F-22 Headed for Reprieve From Congressional Ax." Aviation Week & Space Technology, 9 August 1999.

"Heading Off an 'Electronic Pearl Harbor': CEOs, policy leaders discuss cyber-security at forum." CNN.com, 6 April 1998, n.p. On-line. Internet, 24 December 2001. Available from http://www.cnn.com/TECH/computing / 9804/06/ computer.security/.

Bibliography (Cont.)

"New virus can wipe out hard drives." *CNET.com*, 2 Apr 2000, n.p. On-line. Internet, 26 December 2001. Available from http://news.cnet.com/news/0-1005-200-1623077.html?tag=rltdnws.

"On Course With the New Chief." *Air Force News Agency*, December 1997, n.p. On-line. Internet, December 1997. Available from www.af.mil/news/airman/1297/csaf2.htm.)

"Profile: MGen(S) Michael Hamel--Slow, Steady Path to Success." *Space News*, 21 January 2002.

"Replacing an Aging Fleet." *Government Executive*, 1 August 2001. GovExec.com. On-line. Internet, 1 August 2001, n.p. Available from http://www.govexec.com/top200/01top/s7.htm.)

"SAAS Homepage." Air University website. On-line. Internet, 4 January 2002, n.p. Available from http://www.maxwell.af.mil/au/saas/hist_org.htm.

"Space Acquisition Programs Face 'Serious' Problems, Teets says." *Aviation Week & Space Technology*, 27 Feb 02. On-line. Internet, 28 February 2002. Available from http://www.aviationnow.com/avnow/news/channel_military.jsp?view=story&id=news/steet0227.xml

"Standard & Poor's Industry Surveys." www.sp.com, 15 February 2001, n.p.On-line. Internet,15 July 2001.Available by subscription only.

"The Inflation Calculator." On-line. Internet, 2 Jan 2002, n.p. Available from http://www.westegg.com/inflation/infl.cgi.

"The Posse Comitatus Act: A Principle in Need of Renewal." *Washington University Quarterly*. (Volume 75. Summer 1997 No. 2.), 1.

"U.S. Census Bureau Homepage." US Department of Commerce, 4 Mar 2002. On-line. Internet, 4 Mar 2002. Available from http://www.census.gov/.

"Unites States Intelligence Community." www. cia.gov, 15 June 1998, n.p. On-line. Internet, 30 November 2001. Available from http://www.cia.gov/ic/icagen2.htm

"Unites States Intelligence Community." www. cia.gov, 15 June 1998, n.p. On-line. Internet, 30 November 2001. Available from http://www.cia.gov/ic/icagen2.htm.

"US Coast Guard. The Essence of the Coast Guard: America's Maritime Guardians." In *Joint Force Employment Coursebook Academic Year 2002*. Compiled by Col(s) James Forsyth Jr., PhD, et al. Air Command and Staff College: Department of Joint Warfare Department. Maxwell, AFB, AL. Aug 2001, 24.

"US Shuts Down Somalia Internet." British Broadcasting Company, n.p. On-line. Internet, 23 November 2001. Available from http://news.bbc.co.uk/hi/english/world/africa/newsid_1672000.stm.

"W97M.Melissa.A (also known as W97M.Mailissa) is a typical macro virus which has an unusual payload. When a user opens an infected document, the virus will attempt to e-mail a copy of this document to up to 50 other people, using Microsoft Outlook." (See: Elnitiarta, Raul K. "W97.Melissa.A." *Symantec Security Update,* 29 March 1999, n.p. On-line. Internet, 26 December 2001. Available from www.symantec.com/avcenter/venc/data/mailissa.html.

"War Theory Reflection Questions." *Air Command and Staff College Distance Learning Program*. Lesson TH505. ACSC Multimedia Edited Version 2.2. CD-ROM. August 1997, n.p.

"Worms continue Internet attacks," MSN.com, 25 September 2001, n.p. On-line. Internet, 20 December 2001. Available from http://news.com.com/2009-1001-273186.html?legacy=cnet.

Bibliography (Cont.)

"Worms continue Internet attacks." CNET.com, 25 Sep 2001. On-line. Internet, 26 December 2001, n.p. Available from http://news.com.com/2009-1001-273186.html?legacy=cnet.

5000-2R DoD 5000-2R, "MANDATORY PROCEDURES FOR MAJOR DEFENSE ACQUISITION PROGRAMS (MDAPS) AND MAJOR AUTOMATED INFORMATION SYSTEM (MAIS) ACQUISITION PROGRAMS. 10 Jun 2001.

Abreu, Elinor Mills. "Damage from Code Red worms continuing to add up." *Infoworld.com*, 8 August 2001, n.p. On-line. Internet, 20 December 2001. Available from http://iwsun4.infoworld.com/articles/hn/xml/01/08/08/010808hnredcosts.xml.

Adams, James. *The Next World War*. New York: Simon and Shuster. 1998.

Air Force Doctrine Document 1. *Air Force Basic Doctrine,* September 1997.

Air Force Doctrine Document 2-2. *Space Operations*, 23 August 1998.

Air Force Doctrine Document 2-5.2 Intelligence, Surveillance and reconnaissance Operations, 21 Apr 1999.

Alford, Lionel D. Jr. "Cyber Warfare: A New Doctrine and Taxonomy." On-line. Internet, 12 February 2002, n.p. Available from www.stsc.hill.af.mil/crosstalk/2001/apr/alford.asp.

Arquilla, John and David Ronfeldt. *Networks and Netwars*. RAND: Santa Monica, CA. 2001.

Bates, Jason. "Software Could Lead to Low-Cost Supercomputer." *Space News*, 21 January 2002.

Booz, Allen & Hamilton. "US Defense Industry Under Siege--An Agenda for Change," December 1999. On-line. Internet. Available from: www.aerospacelinks.com.

Butler, Jeffery T. *UAVs and ISR Sensor Technology*. Maxwell AFB, AL: Air Command and Staff College, Apr 2001.

Cahlink, George. "Replacing an Aging Fleet." Government Executive, 1 August 2001. GovExec.com. On-line. Internet, 1 August 2001, n.p. Available from http://www.govexec.com/top200/01top/s7.htm.

Cain, Anthony Christopher. "Neither Decadent, nor Traitorous, Nor Stupid: The French Air Force and Doctrine in the 1930s." Ph.D. Thesis, Ohio State University, 2000.

Campen, Alan D., and Douglas H. Dearth. *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*. AFCEA International Press. Fairfax VA, Oct 200.

Canahuate, Tom. "Analyst Says U.S. Navy Lacks Unifying Transformation Plan."*DefenseNews.com* 16 Jan 2002.On-line. Internet, 18 Jan 2002. Available from http://www.defensenews.com.

Canon, Scott. "Stealth Unmasking Only a Matter of Time." 17 Jun 2001. Kansas City Star.

Chao, Pierre A. "The Structure and Dynamics of the U.S. Defense Industry." Lecture, 18 July 2001. Defense Systems Management College, Fort Belvoir: VA, 26 Jan 2001, 12.)

CJCS 3170.01B. *Requirements Generation System*, 15 Apr 2001.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton NJ: Princeton University Press, 1976.

Costa, Robert. "FFRDCS Evolution As a function of Changing DoD Calculus." Unpublished. Defense Systems Management College, Fort Belvoir: VA, 3 Auf 2002, n.p.

de France, Linda. "Ryan Says Space Force Unwarranted For Next 50 Years." *Aerospace Daily,* 9 Feb 01, n.p. .On-line. Internet, 18 Jan 2002. Available from http://home.datawest.net/dawog/Space/ e20010209 space_force_unwarranted.htm.

Bibliography (Cont.)

De Jomini, Antoine Henri. *The Art of War.* London: Greenhill Press, 1996.

Del Vecchio, Jeffrey R. "An Incentive Model for Secure International Telecommunications." Thesis. Presented to Department of Systems and Engineering Management Graduate School of Engineering and Management Air Force Institute of Technology. Air University. Air Education and Training Command. March 2000.

Department of Defense Office of General Counsel. *An Assessment of International Legal Issues in Information Operations,* May 1999. On-line. Internet, 10 January 2002. Available http://www.terrorism.com/documents/dod-io-legal.pdf..

Department of Defense Office of General Counsel. *An Assessment of International Legal Issues in Information Operations*. Washington D.C.: US Government Printing Office, May 1999.

Echevarria II, Antulio J. "War, Politics, and RMA-the Legacy of Clausewitz." In *Nature of War: NW Coursebook Academic Year 2002*. Compiled by Col(s) James Forsyth Jr., PhD, et al. Air Command and Staff College: Department of International Security and Military Studies. Maxwell, AFB, AL. Aug 2001.

Eisman, Dale. "Navy Criticized For Failing To Reshape Its Role. Norfolk Virginian-Pilot. 17 Jan 2002, n.p.

Elnitiarta, Raul K. "W97.Melissa.A." Symantec Security Update, 29 March 1999, n.p. On-line. Internet, 26 December 2001. Available from www.symantec.com/avcenter/venc/data/mailissa.html.

Ex-pentagon chief targets Defense." 12 Feb 01, n.p. www.Barron.com. On-line. Internet, 12 Jul 2002. Available from www.publiceye.org/frontpage/911/boin.html.

Federal Acquisition Regulation. On-line. Internet, 7 March 2002, n.p. Available from http://www.arnet.gov/far/, 35.0-7.

Festa, Paul and Joe Wilcox. "Experts estimate damages in the billions for bug." CNET.com, 5 May 2000, n.p. On-line. Internet, 20 December 2001. Available from http://news.cnet.com/news/0-1003-200-1814907.html.

Frye, Alton. "Our Gamble in Space: The Military Danger." The Atlantic Monthly, August 1963, n.p. On-line. Internet, 12 Oct 2002. Available from http://www.theatlantic.com/issues/63aug/frye.htm

Fulghum, David A. "Pentagon Champions UAVs, Communications." *Aviation Week and Space Technology*, 17 Dec 2001, n.p. On-line. Internet, 3 February 2001. Available from http://www.aviationnow.com/content/publication/awst/20011217/avi_news.htm.

Fulghum, David A. "Stealthy UAVs Snag Rumsfeld's Attention." *Aviation Week and Space Technology* 4 Jun 01.

Fulghum, David A. and Wall, Robert. "Global Hawk, J-STARS, Head for Afghanistan." *Aviation Week and Space Technology*, 5 Nov 2001.

Gabel, Christopher R. "The Leavenworth Staff College: A Historical Overview." *Military Review*, Sep-Oct 1997, n.p. On-line. Internet, 15 February 2002. Available from http://www-cgsc.army.mil/milrev/□nglish/sepoct97/almanac.htm.

General Accounting Office. *"Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities"*, April 2001. GAO-01-323, April 2001.

General Accounting Office. "Defense Information Security." *www.pbs.org*, May 1996, n.p. On-line. Internet, 20 December 2001. Available from ttp://www.pbs.org/wgbh/pages/frontline/shows/

Bibliography (Cont.)

General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. Report GAO/T-AIMD-96-92, 22 May 96.

General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Testimony of Jack Brock. Report GAO/T-AIMD-96-92*, 22 May 96.

Gildner, Col Will. "JV2020." Lecture. Dept of International Security and Military Studies. Air Command and Staff College. Maxwell AFB, AL, 9 January 2002.

Gingrich, Newt. "Commandant's Speakers Series (CC-812)," lecture, Air Command and Staff College, Maxwell AFB, AL, 6 March 2002.

Grady, John. "Control of Space Crucial in Future Battles." *Army Link News*, 15 December 1997, n.p. On-line. Internet, 20 December 2002. Available from http://dtic.mil/armylink/news/Dec1997/a19971216space.html.

Grier, Peter. "The Winning Combination of Air & Space." *Air Force Magazine Online.* On-line. Internet, 20 February 2002, n.p.. Available from http://www.afa.org/magazine/Jan2002/0102space.html.

Griffin, Major Dwight H. et al. "The Air Corps Tactical School: The Untold Story." *Air Command and Staff College Distance Learning Program*. Lesson TH508. ACSC Multimedia Edited Version 2.2. CD-ROM. August 1997.

Hall, Keith R. "Space Policy, Programs, and Operations." Presentation to the Committee on Armed Services: Subcommittee on Strategic forces," 8 Mar 2000. On-line. Internet, 22 December 2001.Available from http://www.senate.gov/~armed_services/statemnt/2000/000308kh.pdf.

Harnden, Toby. "Rumsfeld Calls For End To Old Tactics Of War." *London Daily Telegraph*, 16 October 2001.

Hart, B.H. Liddell. *Strategy.* New York, New York: Penguin Group, 1991.

Intrusion Detection and Prevention Product Update. Presentation, Cisco Industries. San Jose: CA, 12 Dec 2000. On-line. Internet, 4 February 2002. Available from http://www.cisco.com/networkers/ nw00/pres/2505.pdf.

Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms,* 12 April 2001 (as amended through 15 October 2001).

Joint Publication 3-13. *Joint Doctrine for Information Operations*. Washington, DC., 9 Oct 1998.

Joint Publication 3-33. *Joint Force Capabilities*, 13 October 1999.

Keaney, Thomas A. and Eliot A. Cohen. *Gulf War Air Power Survey Summary Report*. Department of Defense. Washington D.C., 1993.

Kelly, Ricky B. "Centralized Control of Space: The Use of Space Forces by a Joint Force Commander." School of Advanced Airpower Studies. Air University Press. Maxwell Air Force Base, Alabama. 28 June 93.

Kendall, Anthony. "The Creative Leader." In *Leadership and Communication Coursebook Academic year 2002*. Compiled by Col(s) James Forsyth and LtCol Glenn Cobb. Air Command and Staff College: Department of Leadership and Communications Studies. Maxwell, AFB, AL. Aug 2001, 212.Leadership and Command Coursebook.

Khalilzad, Zalmay M. and John P. White. *Strategic Appraisal: The Changing Role of Information in Warfare*. RAND: Project Air Force. Santa Monica, CA: 1999.

Bibliography (Cont.)

Kimery. Anthony. "Moonlight Maze." *MIT-KMI.com,* 3 Dec 99, n.p. On-line. Internet, 20 December 2001. Available fromhttp://www.mit-kmi.com/3_6_art1.htm.

LaSaine, Dr. J. T. Jr. “The Realist Tradition in the United States Foreign Policy.” Lecture. Dept of International Security and Military Studies. Air Command and Staff College. Maxwell AFB, AL, 27 Aug 01.

Link, Maj Gen (ret) Chuck Developing Aerospace Leaders: Presentation to Air Command and Staff College. Maxwell AFB, AL: 17 August 2001.

Loeb, Vernon and Thomas E. Ricks. “l’s And 0’s Replacing Bullets In U.S. Arsenal.” *Washington Post*. 2 February 2002, n.p.

Mahan, Sir Alfred Thayer. “Excerpts from: The Influence of Seapower on World History.” From *The Influence of Seapower Upon History: 1660-1783*, published by Dover Publications, Inc., New York, 1987. In Air Command and Staff College Distance Learning Program. Lesson TH506r01. CD-ROM ACSC Multimedia Edited Version 2.2., Aug 1997, n.p.

Mengxiong, Chang. “The Revolution in Military Affairs: Weapons of the 21st Century.” In *Chinese Views of Future Warfare.* Institute of National Strategic Studies. National Defense University. United States Government Printing Office: Sep 98.

Miller, Michael J. “The Cyberterrorism Threat.” *Pcmag.com*, 27 Nov 2001, n.p. On-line. Internet, 21 December 2001. Available from . Available at http://www.pcmag.com/article/0,2997,s%253D1499%2526a%253D17512,00.asp.

Mitre Homepage, 1 May 2001. On-line. Internet, 28 February 2002. Available from www.mitre.org.

Muller, Dr. Richard R. “The Luftwaffe and Barbarossa, 1941.” In *Airpower Studies: AP Coursebook Academic year 2002*. Compiled by LtCol Micheal Fiedler, Phd, et al. Air Command and Staff College: Department of International Security and Military Studies. Maxwell, AFB, AL: Air University Press, August 2001.

Muradian, Vago. “Air Force Considers Speeding Up C-130J Buy to Control F-22 Cost.” Defense Daily, 23 Oct 99, n.p. On-line. Internet, 2 January 2002. Available from www.d-n-i.net/FCS_Folder.

Myers, Gen. Richard B. “Commander In Chief, U.S. Space Command Testimony Before the U.S. Senate Strategic Forces Subcommittee Senate Armed Services Committee. 22 Mar 1999, n.p..

Parker, Hap. “Air Force secretary shares views on space road map,” *Air Force Link*, 28 November 2001, n.p. On-line. Internet, 20 December 2002. Available from http://www.af.mil/news/Nov2001/ n20011128_1691.shtml.

Paul, Dr. Richard, and Dr. Linda Elder. *The Miniature Guide to Critical Thinking: Concepts and Tools*. Rohnert Park, CA: Foundation of Critical Thinking, 2000.

Pitts, Representative Joseph R. “Electronic-Warfare Assets Badly Neglected.” *National Defense*, June 2000.

Pomfret, John. “China Finds Bugs on Jet Refitted in U.S.” *Washington Post Online*, 19 January, 2002, n.p. On-line. Internet, 3 February 2002. Available from http://www.taiwansecurity.org/WP/2002/WP-011902.htm.)

Bibliography (Cont.)

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* Office of the President. Washington DC: US Government Printing Office, October 1997.

Puffer, Dr. Raymond, L. "The Death of a Satellite," 21 Jun 2001. On-line. Internet, 7 February 2002. Available from www.edwards.af.mil/weekly/docs_html/install-35.html.

Rattray, Gregory J. *Strategic Warfare in Cyberspace.* The MIT Press. Cambridge, MA.

Reynolds, LtCol Joe. "How to Study Things . . . Like Airpower." *Airpower Studies AP Coursebook Academic Year 2002*. Air Command and Staff College Department of International Security and Military Studies. Aug 2001.

Rife P. Shawn, "On Space Power Separatism." In *Airpower Studies: AP Coursebook Academic Year 2002*. Compiled by LtCol Micheal Fiedler, Phd, et al. Air Command and Staff College: Department of International Security and Military Studies. Maxwell, AFB, AL. Aug 2001.

Robinson, Clarence A., Jr. : "China's Military Potency Relies On Arms Information Content." *SIGNAL Magazine*, November1999, n.p. On-line. Internet, 20 Dec 2001. Available from http://www.us.net/signal/Archive/Nov99/china-nov.html.

Rolfsen, Bruce. "On-the-job-testing." *Air Force Times*. 21 Jan 2002..

Seife, Charles. "Where am I?" *Infosec.com*, 19 Mar 2002.. On-line. Internet, 20 December 2002, n.p. Available from http://www.info-sec.com/denial/denial_012298a.html-ssi.

Selinger, Mark. "Senate Panel OK's USAF's 767 Lease Plan." Aviation Week & Space Technology, 5 Dec 01, n.p. On-line. Internet, 1 Jan 2002. Available from http://www.aviationnow.com/avnow/ news/channel_military.jsp?view=story&id=news/m7671205.xml

Shimeall, Timothy, et al. "Countering Cyberwar." *NATO Review*, Winter 2001/2002.

Singer, Jeremy. "Competition Widens But Need for GPS 3 Questioned." Space News, 18 February 2002.

Sirak, Michael. "USAF Plans 'Space Control." *Jane's Defence Weekly*, 31 Oct 01, n.p. On-line. Internet, 20 December 2002. Available from http://131.84.1.68/Jan2002/e20020108roche.htm.

Smith, James M. "USAF Culture and Cohesion: Building and Air and Space Force for a 21st Century." Institute for National Strategic Studies. Occasional Paper 19. Colorado Springs, CO: USAF Institute for National Security Studies, June 1998.

Statement of Congressman Pitts, Joseph R. "Surveillance and Support: Shortfalls in Electronic Warfare, 9 Sep 99.

Sweetman, Bill. "Stealth Threat." *Popular Science*. Dec 2001, n.p. On-line. Internet, 8 Feb 2002. Available from http://www.popsci.com/popsci/aviation/article/0,12543,188700-1,00.html.

The White House. *A National Security Strategy for a Global Age*. Washington DC: Office of the White House, December 2000.

Thompson, Dr. Loren B. "US Must Reverse Bomber Blueprint, Air Force Dominated by tactical fighter community, experts say." National Defense. July/Aug 1999. On-Line. Internet, Available from http://www.lexingtoninstitute.org/defense/revbmb.htm.

Thompson, Loren B, Phd. *Rumsfeld's Challenge: Does this Ship Turn.* Briefing. Lexington, MA: Lexington Institute, August 2001.

Bibliography (Cont.)

Thompson, Loren B., PhD. "The Future of Airborne Electronic Warfare." Lexington Institute. Available ON-line Internet. http://www.navyleague.org

Tirpak, John A. "The New World of Information Warfare." Air Force Magazine, 1996. On-line. Internet, 20 Dec 2001. Available from http://www.afa.org/magazine/toc/06cont96.html, n.p.

Turner, Capt David A. "Bullet Background Paper On UAV Comm Issues." Bullet Background Paper, AC2ISRC, 30 Mar 00.

Tzu, Sun. *The Art of War*. Edited and translated by Samuel B. Griffith. New York: Oxford University Press: 1971.

U.S. Department of Defense. *Joint Vision 2020*. Washington DC: US Government Printing Office, Jun 2000.

Unified Command Plan: For Instructional Purposes. NP Coursebook. 29 Sep 1999.

US Department of Defense. *Quadrennial Defense Review Report*. Washington DC: U.S. Government Printing Office, Sep 2001.

US Department of Defense*. Report to Congress Pursuant to the FY2000 National Defense Authorization Act: U.S. Report on China's Military Power (2000)*. Washington D.C.: U.S. Government Printing Office, 2000.

US Department of Defense. *Report to Congress. Kosovo/Allied Force After Action Report.* Washington D.C.: U.S. Government Printing Office, 31 Jan 2000.

US Government. "Inherent Government Functions." PDD 92-1.

US House. *HEARING NOTICE: Transforming the IT and Acquisition Workforces: Using Market-Based Pay, Recruiting and Retention Strategies to Make the Federal Government an Employer of Choice for IT and Acquisition Employees.* 101st Congress, Subcommittee on Technology and Procurement Policy, 2 Oct 01. n.p.

Vasquez, John A. "Conceptualizing War." In Nature of War: NW *Coursebook Academic Year 2002*. Compiled by Col(s) James Forsyth Jr., PhD, et al. Air Command and Staff College: Department of International Security and Military Studies. Maxwell, AFB, AL, Aug 2001.

Wall, Robert. "Costs Cast Shadow On F-22 Go-Ahead." Aviation Week & Space Technology, 3 August 2001, n.p.

Weinberger, Sharon. "Intelligence, Surveillance, Reconnaissance Assets 'Woefully Short,' Says USAFE Commander." *Aerospace Daily*. 25 Jan 2002, n.p.

Widnall, Sheila E. "The Space and Air Force of the Next Century." Presented at the National Security Forum, Maxwell Air Force Base, AL, 29 May 1997.

Wilde, LCDR Andy "Update: Information Operations: A common Perspective." *USACOM Joint Warfighting Center's Newsletter 6*, No. 2 (October 1998.)